University of New South Wales Law Research Series

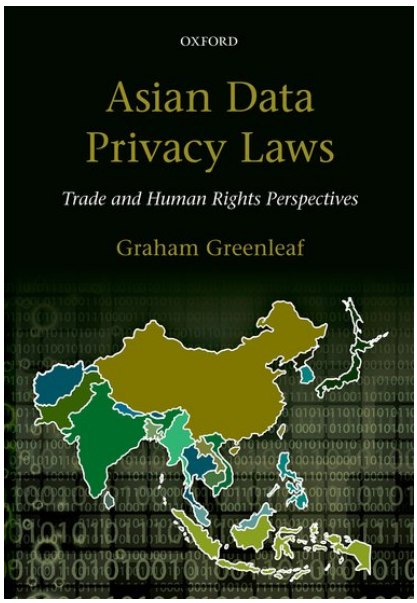
2014-2017 Update to Graham Greenleaf's Asia Data Privacy Laws – Trade and Human Rights Perspectives

GRAHAM GREENLEAF

[2017] *UNSWLRS* 47

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html



2014-2017 Update to Graham Greenleaf's *Asian Data Privacy Laws – Trade and Human Rights Perspectives*

(Oxford University Press, 2014; Paperback edition 2017)

This is an update from mid-2014 to mid-2017 of my *Asian Data Privacy Laws – Trade and Human Rights Perspectives* (Oxford University Press, 2014), to accompany the publication of the paperback edition in July 2017. Purchase details and reviews are on the OUP website.[1]

This update is organized according to the Chapter structure of the book, as set out in the following Table of Contents. Although some content has been written specifically for this Update, in other cases the content consists of abstracts of articles I have authored or co-authored since mid-2014 when the book was published, and links to those articles. Some links are to articles by colleagues, and assistance received in preparing this update is acknowledged with gratitude.[2] The links are located in the footnotes. For each chapter or section, updates are in chronological order.

The important thing to remember in using this update is that only abstracts of these articles are included: it is necessary to go the articles (available for free access on SSRN and elsewhere) to obtain the details. Also, the update is intended to be read in conjunction with the 2014 book, and does not repeat information that can be found there.

This update aims to cover developments to 30 June 2017. While I may periodically update this document, if readers wish to keep up with further developments, a subscription to *Privacy Laws & Business International Report (PLBIR)*[3] is recommended.

Graham Greenleaf
Professor of Law & Information Systems, UNSW Australia
Asia-Pacific Editor, Privacy Laws & Business International Report (PLBIR)
30 June 2017

---

[1] OUP website: https://global.oup.com/academic/product/asian-data-privacy-laws-9780198810094?lang=en&cc=au

[2] The assistance is acknowledged of Scott Livingston, Elonnai, Hickok, Andin Aditya Rahman, Sonny Zulhuda, Clarisse Girot, Hui-ling Chen, Michael R. Fahey, Whon-il Park and Jill Matthews. Assistance with particular articles is acknowledged in those articles. All content is the responsibility of the author. Thanks also to *Privacy Laws & Business*, and particularly to Stewart Dresner and Laura Linkomes.

[3] PLBIR website https://www.privacylaws.com/Publications/int/.

Table of Contents – by book chapter

PART I. ASIA AND INTERNATIONAL DATA PRIVACY STANDARDS

1. Data Privacy Laws in Asia—Context and History

The whole of Chapter 1 'Data Privacy Laws in Asia – Context and History' of *Asian Data Privacy Laws – Trade and Human Rights Perspectives* (Oxford University Press, 2014) is available for download.[4]

There are no specific updates for this Chapter, because the overall assessment of development over the past three years from mid-2014 to mid-2017 is in the update to Chapter 20.

2. International Structures Affecting Data Privacy in Asia

International agreements generally

This article gives an overview of recent developments of global significance:

G. Greenleaf, International Data Privacy Agreements after the GDPR and Schrems (2016) 139 Privacy Laws & Business International Report 12-15.[5] Now that the content of the EU's General Data Protection Regulation (GDPR) has substantially been settled, and the *Schrems* decision of the European Court of Justice has confirmed the parameters within which both it and the existing EU data protection Directive of 1995 must be considered, what are the implications for international agreements affecting data privacy? This brief article aims to sketch the larger picture, by focusing on five developments.

(i) Council of Europe (CoE) data protection Convention 108 of 1981 is strengthening its position as the emerging global data privacy agreement, but there remain unresolved issues in its operation. A quiet development with long-term significance is that the European Union is now more strongly supporting Convention 108 as a global privacy treaty, and has demonstrated this in three ways. The globalisation of Convention 108 is accelerating, with three new invitations to accede (to Mauritius, Senegal, and Tunisia) being issued in 2015. However, a problem with the existing Convention 108 is that its 'conditions of membership' only requires a Party to 'take the necessary measures in its domestic law to give effect' to the principles in the Convention, and do not involve any investigation of the effective enforcement of the law. This deficiency is expected to be remedied in the 'Modernisation' of Convention 108, which is to be finalised following the completion of the EU's General Data Protection Regulation (GDPR).

(ii) The EU's data protection Directive still has life in it until late 2018. This article explains how adequacy assessments made under the Directive will be dealt with until the GDPR. It also includes a first assessment of which elements of the GDPR, and the 'modernised' Convention 108, might constitute a '3rd generation' of data privacy standards.

(iii) Trade agreements play an increasingly important role in the privacy landscape, and here the *Schrems* decision is likely to affect the EU's position in negotiations with the US concerning the Transatlantic Trade and Investment Partnership (TTIP). The EU's negotiating position on the TTIP has been disclosed, following disquiet with

[4] https://ssrn.com/abstract=2514972

[5] https://ssrn.com/abstract=2764864

secret negotiations, and is much the same as in the GATS provision. If the EU maintains such approaches in the TTIP negotiations (and in other FTA negotiations), it will be providing a less privacy-hostile alternative for FTA development than has emerged from the Trans-Pacific Partnership (TPP) text.

(iv) According to the *Schrems* decision, the EU-US 'Privacy Shield' now proposed to replace the illegal 'Safe Harbor', 'must provide a level of protection of fundamental rights essentially equivalent to that guaranteed within the EU under the directive read in the light of the Charter.' The US Judicial Redress Act is a necessary part of US efforts to achieve that goal.

(v) APEC's privacy instruments continue to play a minor but increasing role.

Post GDPR, the most important influences in the global development of privacy standards remain European (both EU and Council of Europe). Their most significant challenge continues to come from the United States, increasingly from its ability to shape the Free Trade Agreements that threaten to cripple data export restrictions. A Great Game of 40 years continues.

EU adequacy assessments

Both Japan and South Korea have sought EU assessments of the adequacy of their data protection regimes, which assessments are ongoing. The details are in the respective country chapters of this update. India's most recent adequacy assessment, conducted in 2013, did not proceed to a positive finding. In January 2017 in its Communication[6] on Exchanging and Protecting personal data in a globalised world, the Commission has launched a dialogue with the aim of reaching an "adequacy decision" with Japan and with South Korea. In light of *Schrems*, adequacy decisions must be based on allowing the free flow of personal data to countries with 'essentially equivalent' data protection rules to those in the EU.

Council of Europe data protection Convention 108 accession

Some Asian countries are also considering an alternative 'globalisation' option: Japan, South Korea, Indonesia and the Philippines have all become observers on the Consultative Committee of Council of Europe data protection Convention 108, and might be eligible to accede to the Convention. Singapore, Malaysia and Vietnam would not be eligible because their data privacy laws do not cover their public sectors. Taiwan could not do so because it does not have a DPA. It would be complex for Hong Kong or Macau to join because they are not countries.

APEC CBPRs

G. Greenleaf, APEC's Cross-Border Privacy Rules System: A House of Cards? (April 20, 2014). (2014) 128 Privacy Laws & Business International Report, 27-30.[7] APEC's Cross-border Privacy Rules system (CPBRs) has been under development at least since 2007, after the APEC Privacy Framework was completed in 2005. The proponents of APEC CBPRs present it as having a major role in the Asia-Pacific, and in transfers of personal data globally, particularly between the EU and the Asia-Pacific. Different views are possible, but it needs to be examined and debated in considerable detail. I suggest scepticism, and that APEC CBPRs may turn out to be a house of cards. The article starts by noting that the EU's Article 29 Working Party Opinion in February 2014 in the form of a 'referential' on EU BCRs (Binding Corporate Rules) and APEC's CBPRs does not aim at achieving mutual recognition of the two systems but only 'a basis for double certification'. There are such wide differences between

[6] European Commission 'Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions', 10 January 2017 < http://europa.eu/rapid/press-release_IP-17-16_en.htm>

[7] https://ssrn.com/abstract=2468782

the two, identified in the Opinion, that a lengthy period of study is required even to understand them, let alone build bridges to overcome them. In contrast, a report by a consultancy firm concludes, with what seems unjustifiably optimistic, when read against the Working Party's later Opinion, that these differences can be overcome, and a resulting global system for 'low friction cross-border transfers' (otherwise known as 'interoperability') can emerge based on something resembling APEC's CBPRs. These contrasting studies make clear is that it is necessary for businesses and their advisers to obtain a very clear and detailed understanding of what APEC CBPRs does and does not do, and the foundations on which it is built. This article aims to provide such an analysis, in a 12 point summary of how APEC CBPRs is supposed to work, followed by a critique of the limited (if any) benefits it will provide for consumers, and the dubious business case it presents for any businesses, other than perhaps a small number of US-based companies.

Greenleaf, Graham, Japan Joins APEC-CBPRs: Does It Matter? (2016) 144 Privacy Laws & Business International Report, 18-21.[8] Japan stepped up its involvement in APEC's CBPRs during 2016. After signalling its intention to join CBPRs in 2013, it did not take the final step until February 2016, when it appointed an 'Accountability Agent' (AA), the Japan Institute for Promotion of Digital Economy and Community (JIPDEC), a trustmark provider. Then in November 2016, Japan's Personal Information Protection Commission (PIPC) announced a decision under Japan's Amended Act on the Protection of Personal Information (PIPA) to the effect that APEC CBPRs compliant 'business operators' are not required to comply with the Act's restrictions on exports of personal data from Japan. This article examines which (if either) of these two developments are important, and to whom? In doing so, it may explain something about the extreme limitations of the APEC CBPRs system that are contrary to how it is presented by its promoters, who give rosy assurances of its success and expansion.

The conclusions reached by the article are that:
(i) The fact that Japan has fully joined APEC CBPRs, by appointing JIPDEC as an AA, will mean nothing of any significance to anyone, even when JIPDEC does some accreditations, because Japan already has a data privacy law with higher standards than APEC. In contrast, the US CBPRs participation is of some effect, because it does not have data privacy laws meeting APEC standards (low as they are).
(ii) However, the 'recognition' of CBPRs accreditation in overseas countries by Japan's PIPC is significant, though its practical effect is as yet limited to facilitating data exports to a handful of businesses in one country, the US.

While APEC CBPRs' significance is limited to only a small number of US companies, and to no-one else, it will remain irrelevant, provided its limitations are understood.

2016-17 APEC CBPRs developments: In December 2016 South Korea lodged its *Notice of Intent to Participate in the CBPR System*, and APEC's Joint Oversight Panel (JOP) has approved its participation.[9] As with Canada and Mexico, Korea has to choose an APEC-approved Accountability Agent before its participation is complete. Taiwan has stated that it 'hopes to participate'.[10] CBPRs has had no impact on ASEAN countries as yet. None of the seven ASEAN countries which are APEC members have taken any of the formal steps to join CBPRs. Although a report prepared by Vietnam in late 2016 claimed that the Philippines 'planned to

[8] https://ssrn.com/abstract=2964499

[9] APEC CBPRs JOP JOP Findings Report regarding Korea's intent to participate in the CBPR system, 1 June 2017 <https://cbprs.blob.core.windows.net/files/JOP%20Findings%20Report_Korea_FINAL.pdf>.

[10] Taiwan Executive Yuan Taiwan's achievements during 2016 APEC Economic Leaders' Week', 8 December 2016 <http://english.ey.gov.tw/News_Hot_Topic.aspx?n=9CAC6D643D2B87F8&sms=C7706D6F9D246174>

join', and Singapore and Vietnam were 'considering' doing so, no letter of intent from any of these countries has yet appeared on the APEC CBPRs website.[11] Malaysia was reported to have 'no plan to join', and the other ASEAN countries had no laws enabling them to do so.[12]

The administration of APEC CBPRs continues to raise questions. The US Federal Trade Commission (FTC) settled allegations that three companies falsely claimed they participated in APEC CBPRs.[13] TRUSTe, the US Accountability Agent for CBPRs, agreed to pay US$100,000 as settlement to the New York Attorney General's Office, for its failure to determine, as required, whether customers of its certification program did in fact comply with the US COPPA (children's privacy) legislation.[14]

A number of Asian countries are involved in APEC's Cross Border Privacy Enforcement Arrangement (CPEA), which is separate from APEC CBPRs, but a pre-condition for involvement.

Free Trade Agreements (FTAs)

G. Greenleaf, The TPP & Other Free Trade Agreements: Faustian Bargains for Privacy? UNSW Law Research Paper No. 2016-08.[15] Free Trade Agreements (FTAs) are not likely to be sources of privacy rights, but may act as limitations on the operation of privacy laws. Countries negotiating new bilateral or multilateral trade agreements, particularly, but not exclusively, the USA, are likely to attempt to include a requirement that the parties do not include any significant data export restrictions, or 'data localisation' provisions in their laws. I argue that, in most cases, the only role that privacy rights should play in Free Trade Agreements is a negative one: as explicit exceptions confirming that other FTA provisions have nothing to do with limiting the protection of privacy (or other human rights). Human rights are not bananas, to be traded for other commodities. Until 2016, Article XIV(c)(ii) of the GATS (General Agreement on Trade in Services, 1995) was the only significant privacy limitation in FTAs, but an important one because of its near-universality. Its effect is still uncertain, as it has not yet resulted in WTO case law.

The Trans-Pacific Partnership (TPP) agreement, signed (but not ratified) in February 2016, is the first multilateral trade agreement with detailed provisions relating to privacy/data protection that go beyond GATS, and they are overwhelmingly negative from a privacy perspective. The TPP requirements involve: (a) no substantive or meaningful requirements to protect privacy; (b) coupled with prohibitions on data export limitations or data localisation requirements that can only be overcome by a complex 'four step test' of justification; and (c) backed up by the risk of enforcement proceedings between states or under ISDS provisions, both involving uncertain outcomes from dubious tribunals and potentially very large damages claims. TPP seems to be the type of binding international privacy treaty that the USA (in particular) wishes to achieve. For the other states whose personal data will be 'hoovered up', it is more likely to be a Faustian bargain: put at risk the protection of the privacy of your citizens (except at home) in return for the golden chalice of trade liberalisation. If the TPP is defeated in the US Congress, this will be a net gain for privacy protection, whatever one thinks

---

[11] APEC 'CBPR system documents' <http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx>.

[12] 'Survey on the Readiness for Joining Cross Border Privacy Rules System – CBPRs', APEC Electronic Commerce Steering Group (ECSG), January 2017 <http://publications.apec.org/publication-detail.php?pub_id=1800>.

[13] US Federal Trade Commission (FTC) 'Three Companies Settle FTC Charges that They Deceived Consumers About Participation in International Privacy Program' 22 February 2017 https://www.ftc.gov/news-events/press-releases/2017/02/three-companies-settle-ftc-charges-they-deceived-consumers-about >.

[14] Manatt Phelps & Phillips LLP 'TRUSTe Will Pay $100,000 in Deal Over COPPA Violations' *Lexology* 27 April 2017.

[15] https://ssrn.com/abstract=2732386

about the other potential economic advantages of the TPP. [*Postscript:* President Trump withdrew the US from the TPP in early 2017, so it did not go before the Congress.]

In the meantime, other FTAs are proliferating, and overlapping in confusing ways. This article concludes with a review of what (if anything) is known of possible privacy provisions in agreements under negotiation including the EU-US TTIP, the Trade in Services Agreement (TISA), RCEP, and PACER. One way or another, FTAs are likely to be one of the defining factors in the future evolution of data privacy laws.

2017 FTA developments: The Regional Comprehensive Economic Partnership (RCEP), is a trade agreement covering ten members of ASEAN and six partner countries – China, India, Japan, Australia, New Zealand and South Korea. RCEP is its most likely successor to the defunct Trans-Pacific Partnership (TPP), which posed great dangers to all data privacy laws through its prohibitions on personal data export limitations and data localisation[16]. Whether RCEP contains similar restrictions, or anything else affecting data privacy, is not certain because of the secrecy surrounding drafts and negotiations,[17] but the most recent leaked version of the draft chapter on Trade in Services (August 2015)[18] does not include any provisions concerning these matters. The 18th round of negotiations were held in the Philippines on 2-12 May 2017. Perhaps the fact that the US is not involved in RCEP, unlike the TPP, will produce a better result for privacy. Attempts are also being made by some countries to revive the TPP, without US participation, which will require re-negotiated treaty terms.

ASEAN

The ten ASEAN (Association of South East Asian Nations) member states include some of the world's most rapidly-developing economies, and have high ambitions for economic integration. The ASEAN Economic Community (AEC),[19] established in 2015, has as one of its e-commerce objectives[20] the development in 2016-2025 of a 'coherent and comprehensive framework for personal data protection', including 'Regional Data Protection and Privacy Principles'.

In November 2016 the Telecommunications and IT Ministers of the ASEAN member states adopted the *ASEAN Framework on Personal Data Protection*[21]which is a non-binding "record of Participants' intentions" with no practical effects and no obligations concerning implementation. It refers to the APEC Privacy Framework, and includes principles similar to those APEC principles, but with the addition of a principle concerning cessation of retention of personal data.

---

[16] Greenleaf, Graham, The TPP & Other Free Trade Agreements: Faustian Bargains for Privacy? 14 February, 2016 (pre-publcation draft) <https://ssrn.com/abstract=2732386>; in Dan Svantesson and Dariusz Kloza *Transatlantic Data Privacy Relationships as a Challenge for Democracy* (European Integration and Democracy series) (Intersentia, 2017).

[17] Jyoti Panday 'RCEP's Digital Trade Negotiations Remain Shrouded in Secrecy', 16 May 2017 <https://www.eff.org/deeplinks/2017/05/rcep-negotiations-remain-shrouded-secrecy>.

[18] Bilaterals.org 'RCEP - draft chapter on trade in services' August 2015 <http://www.bilaterals.org/IMG/pdf/services_consolidated_text_-_5aug2015-2.pdf>.

[19] ASEAN Economic Community (AEC) website <http://asean.org/asean-economic-community/>

[20] *ASEAN Economic Community 2025 Consolidated Strategic Action Plan*, February 2017 <http://asean.org/storage/2012/05/Consolidated-Strategic-Action-Plan-endorsed-060217rev.pdf>; Endorsed by the AEM and AEC Council on 6 February 2017.

[21] 'ASEAN Framework on Personal Data Protection' <http://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf>

Regional associations

ASEAN and the broader Asian region have a number of active multinational business and NGO initiatives concerning data privacy, as well as an association of data protection authorities.

The *Asia-Pacific Privacy Authorities* (APPA), an association of DPAs, now has 18 members from 10 countries (largely the same as countries in APEC), with Japan's DPA being its most significant new member.

Academics and NGO representatives in the broader Asian region have successfully established the *Asian Privacy Scholars Network* (APSN), now with over 110 members.[22]. Founded in 2010, APSN will hold its sixth conference in Hong Kong in September 2017.

The *Asian Business Law Institute* (ABLI), an initiative of the Singapore Academy of Law, was launched in January 2017.[23] ABLI has initiated a multi-stakeholder project on provisions concerning cross-border data flows in Asian jurisdictions (including India and China, intending to make recommendations for the convergence of these. It is organizing reporters from each jurisdictions, and an experts committee comprising regulators, practitioners, academics and industry representatives.

3. Standards by Which to Assess a Country's Data Privacy Laws

There are no updates to this Chapter because there are no new international agreements since 2014 which are as yet in force. Both the EU's General Data Protection Regulation (GDPR), which will be in force in 2018, and the 'modernised' Council of Europe Convention 108 do provide new, and stronger, candidate international standards than their predecessors, both in relation to data privacy principles and to enforcement mechanisms. However, because neither are yet in effect it is premature to assess which aspects of their 'candidate standards' will in fact become international standards due to their inclusion in what is regarded as necessary for EU 'adequacy' assessments, access to Convention 108, and adoption in legislation outside Europe.

G. Greenleaf, International Data Privacy Agreements after the GDPR and Schrems (2016) 139 Privacy Laws & Business International Report 12-15[24] includes an initial assessment of which elements of the GDPR, and the 'modernised' Convention 108, go beyond the 'European standards' considered in this chapter, and might over time constitute part of a '3rd generation' of global data privacy standards.

---

[22] Asian Privacy Scholars Network (APSN) <http://asianprivacy.org/>.

[23] Asian Business Law Institute <http:///www.abli.asia>; ABLI has a fourteen member Board of Governors drawn from the judiciary, academia and practitioners from Singapore, China, India, Australia and other jurisdictions. It aims to address key problems resulting from the considerable heterogeneity that exists among Asian legal systems.

[24] https://ssrn.com/abstract=2764864

PART II. NATIONAL DATA PRIVACY LAWS IN ASIA

4. Hong Kong SAR—New Life for an Established Law

A new Privacy Commissioner for Personal Data (PCPD), Mr Stephen Kai-yi Wong, was appointed in August 2015, the fifth Commissioner under Asia's longest-operational comprehensive data privacy law. The PCPD continues to be very active in issuing numerous guidelines and engaging with the Hong Kong community in relation to the operation of the Ordinance, and public issues that arise.[25]

Enforcement

G. Greenleaf, Hong Kong Data Privacy 2015: Cautious Enforcement, Strong Principles (2015) 138 Privacy Laws & Business International Report, 21-23.[26] For seventeen years, Hong Kong's 1995 Personal Data (Privacy) Ordinance, the first comprehensive data privacy law in Asia, remained without substantial amendments. The Amendment Bill of 2012, in force since April 2013, involved fewer changes than were recommended by Hong Kong's Privacy Commissioner, but were nevertheless a significant strengthening of the Ordinance. Two and half years later, the stronger enforcement regime is still only being applied cautiously. However, the Commissioner and the tribunal administering the Ordinance have both given its substantive principles increasingly strong interpretations. This article reviews these developments. Aspects covered include the first direct marketing fines, the first jail sentence, the appeal decision upholding coverage of publicly available information, decisions concerning collection by unfair means and limits on excessive collection, and legislation on third party rights under contracts.

2016-17 Hong Kong developments: In June 2017, PCPD published its first investigation report under s. 48(2) since 2015 (see above article). It concerned the loss of two notebook computers Registration and Election Office (REO), containing personal data of election committee members (the first computer) and 3.78 million electors (the second computer), reported to PCPD the day after Hong Kong's 2017 Chief Executive Election. The details on electors included their HK ID numbers, considered to be sensitive personal data. Concerning the second computer, the Commissioner found there was a breach of the Ordinance, and issued an enforcement notice to the REO. This primarily concerned the assessment and approval of the use of an enquiry system containing the electors' data because 'the security measures adopted by the REO were not proportional to the degree of sensitivity of the data and the harm that might result from a data security incident either'. Among a very detailed list of requirements, Privacy Impact Assessments will be required before any changed uses of data in future.[27]

---

[25]For many examples, see PCPD (HK) 'Media Statements and Responses' <https://www.pcpd.org.hk/english/news_events/media_statements_responses/index.html?year=2017>.

[26] https://ssrn.com/abstract=2733882

[27] PCPD (HK) 'Privacy Commissioner Publishes Investigation Report on the Loss of Registration and Electoral Office's Notebook Computers containing Personal Data of Election Committee Members and Electors' 12 June 2017 <https://www.pcpd.org.hk/english/news_events/media_statements/press_20170612.html > ; the Investigation Report is at 'https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/PCPD_Investigation_Report_R17-6429_Eng.pdf

'Name and shame' as an enforcement technique in relation to the private sector is therefore not yet being used by the current Commissioner. Other visible aspects of enforcement on the PCPD website have become very limited. Only one new casenote (complaint summary) has been published since 2015. Summaries of court decisions since 2013 are not included, although some examples of minor prosecutions of breaches are included in the 'News' section. There are no summaries of appeal cases to the Administrative Appeals Board since 2014. While the visibility of the PCPD remains high, the transparency of its enforcement activities no longer appears to be quite as strong.

Guidance Notes - Data exports and others

PCPD has continued since 2014 to issue new non-binding *Guidance Notes*,[28] namely Guidance on Personal Data Protection in Cross-border Data Transfer (December 2014); Guidance on Collection and Use of Biometric Data (July 2015); Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Healthcare Providers and Healthcare Professionals) (February 2016); and Guidance on the Proper Handling of Customers' Personal Data for the Beauty Industry (June 2016). Many existing Guidance Notes have also been revised.

5. South Korea—The Most Innovative Law

The following areas of change to Korea's data privacy regime since 2014 are significant: amendments to the Network Act and the Personal Information Protection Act; stronger enforcement laws and penalties under all Acts; 2016 de-identification guidelines; 2015 cloud computing law; and international engagement.

International engagement

Korea's plans concerning greater international engagement in relation to its data privacy laws, involve interactions with the EU, Council of Europe and APEC. Korea has announced that it wishes to obtain an 'adequacy' assessment from the EU, and has taken the novel approach of preparing a detailed 'self-assessment' report on the strengths and remaining weaknesses of Korea's data protection regime, which it presented to the EU in 2016.[29] Korea updated this self-assessment report in 2017, and the EU has stated that this is one of the adequacy assessments to which it is giving priority. In 2017 Korea became an observer on the Consultative Committee of Council of Europe Convention 108, and attended its annual Plenary meeting. In December 2016 South Korea lodged its *Notice of Intent to Participate in the CBPR System*, and APEC's Joint Oversight Panel (JOP) has approved its participation.[30]

There is, since 2016, a Personal Information Protection Portal,[31] with an English language section. Translations of the most important Acts (but not the enforcement decrees), and some policies (eg de-identification/big data Guidelines) are provided. It includes a valuable selection of summaries of cases from the Constitutional Court, Supreme Court and lower courts, but they do not include all important cases.

---

[28] PCPD (Hong Kong) 'Guidance Notes' <https://www.pcpd.org.hk/english/resources_centre/publications/guidance/guidance.html>

[29] The author was a member of the committee which prepared the 2016 report to the EU for KISA. This update includes some extracts from that report which were written by the author.

[30] APEC CBPRs JOP JOP Findings Report regarding Korea's intent to participate in the CBPR system, 1 June 2017 <https://cbprs.blob.core.windows.net/files/JOP%20Findings%20Report_Korea_FINAL.pdf>.

[31] Ministry of Interior (Korea) 'Personal Information Protection Portal' <http://www.privacy.go.kr/index.jsp>, with English version 'Personal Data Protection Laws in Korea' <https://www.privacy.go.kr/eng/>. Some browser software says the site is improperly configured and may be a security risk.

Korea's personal data export restrictions are still based on consent of the data subject, rather than having any relationship to the protections provided in the destination county or by the recipient. The Korean government has indicated an intention to change this aspect of its laws but has not yet done so.

Principles

The Personal Information Protection Act (PIPA) defines 'personal information' to mean 'any information which relates to a living natural person who can be identified or identifiable from those data including name, resident registration number and image, etc. (including the information that does not, on its own, permit direct identification of a specific individual, but that does identify specific individual when it is easily combined with other information' (art. 2).[32] The definition in the Network Act, Art. 2, is similar.

The inclusion of the word 'easily' means that Korea does not have a conventional definition of 'personal information'.[33] Instead, it has a more narrow definition because if a data item cannot be 'easily' combined with other data to identify an individual, then it is not 'personal information', and it remains unregulated by Korean data privacy laws. This difference is important to Korea's current policies on 'big data'.

'Big data' / de-identification Guidelines

The Korean Communications Commission (KCC) had released 'Big Data Guidelines for Data Protection' in December 2014.[34] In July 2014, the Personal Information Protection Commission (PIPC), had advised KCC that the draft guidelines did not conform to existing law, and advised reconsideration.

In 2016 a consortium of Korean ministries and commissions[35] including KCC, FSC and MOI (but not including the PIPC), released the *Guidelines for De-identification of Personal Data.*[36] The 2014 Guidelines, and a number of ministerial regulations, were repealed.[37]Like their predecessor, the new Guidelines do not have any clear legal status. It does not appear that they are legally binding, nor that they would in themselves protect organisations against possible actions for breaches of any of Korea's data protection laws. However, given that the Guidelines have been issued by all of the main organisations enforcing these laws – KCC, FSC and MOI – companies operating in Korea may reasonably question whether any enforcement actions would be taken against them for following the Guidelines by these bodies. Nevertheless, there is still the possibility of court actions independent of these enforcement bodies. The legal effect of the Guidelines is therefore unresolved.

The purpose of the Guidelines includes to 'provide standards for businesses which intend to use or provide de-identified personal data' (II-1). The Guidelines do not only focus on the

---

[32] The English translation of PIPA on the official English language portal now includes the phrase 'when it is easily combined with', but until March 2017 it instead stated 'if combined with'. Pre-2017 commentary must therefore be read with care.

[33] For example, the 1995 EU data protection Directive, Art. 2(a) states " 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity;"

[34] For a summary of these 2014 Guidelines, see Kwang-Bae Park and Hwan-Kyoung Ko, 'Highlights of the "Big Data Guidelines for Data Protection" ', Lee & Ko Data Protection / Privacy Newsletter, January 2015 <http://www.leeko.com/data2/publication/Newsletter%20-%20January%202015(4).htm>;

[35] Office for Government Policy Coordination; Ministry of Interior; Korea Communications Commission; Financial Services Commission; Ministry of Science, ICT and Future Planning; and Ministry of Health and Welfare

[36] Interdepartmental Joint Announcement *Guidelines for De-identification of Personal Data* (Korea), 30 June 2016 <https://www.privacy.go.kr/eng/news_event_view.do?nttId=7585>

[37] Details are in Whon-il Park 'Big Data Guideline' (KoreanLII) < http://www.koreanlii.or.kr/w/index.php/Big_Data_Guideline> .

process of de-identification, because, even when personal data is held to be de-identified, numerous obligations in relation to its management are intended to continue.

The 'preliminary review' step (II-2(1)) involves determining 'whether specific data is personal data or not', because if it is not 'it can be used for big data analysis without additional measures'. The key question in relation to determining whether it is personal data is whether it is 'data that can be easily combined with other data when given data is not enough to identify a specific person'. The inclusion of the word 'easily' in the definition of 'personal information' is clearly at the heart of these Guidelines. The Guidelines say "'easy combination with other data' means that it should be possible to obtain other information to be combined and there is a high possibility of combining with other information," and this 'does not include data that can't be legally collected and requires irrational amount of time or costs for collection' (II-2(1)B(e)).

If data is held to be 'personal data' under (II-2(1)), then step (II-2(2)) involves applying 'de-identification models' (or standards) in relation to identifiers and attribute values, both of which should where possible be removed. A range of methods of de-identification are suggested (pseudonymization; aggregation; data reduction; data suppression; and data masking). After this de-identification of personal data is completed, an 'adequacy assessment' of its sufficiency must be carried out using a 'k-Anonymity model' 'among other privacy protection models' (II-2(3)). 'Adequacy assessment procedures' including a Privacy Officer and 'external professionals' are specified.

Once the adequacy of the de-identification is determined, 'data can be used or provided for big data analysis' (II-2(3)-5). In Data Utilization, the following steps are still required: (i) Provision to the public is generally prohibited, because of re-identification risks, except if pursuant to relevant laws (eg Act on Promotion of the Provision and Use of Public Data); (ii) Immediate destruction of data 'once the purpose of using data is fulfilled or it is no longer needed'; and (iii) 'follow-up management' ((II-2(4))) including prohibiting sharing of data likely to increase re-identification risks, and making contingency plans 'for possible leakage of de-identified data'. There must also be regular monitoring and testing for possibilities of re-identification, and taking of further steps if needed. Contractual measures are specified for when de-identified data is provided to a third party, as well as re-identification counter-measures. It is clearly intended that, even where personal data is held to be de-identified, numerous obligations in relation to its management remain.

Legal sanctions are specified which may apply if re-identification occurs (III-3), but otherwise the Guidelines do not include any analysis of how these Guidelines are consistent with any of Korea's data privacy laws, including their relationship to collection of personal data for particularly purposes, or consent to additional uses. The legal position is complex and ambiguous, and cannot be resolved here.

Amendments to PIPA, and role of PIPC

Korea's Personal Information Protection Commission (PIPC) has had a limited role in any of the recent developments, and is not the equivalent of a data protection authority (DPA) under European-style laws.[38] It is only one policy and enforcement body among others (KCC, KISA, MOI etc).

The 2015 amendment to PIPA (effective on July 25, 2016) gave broader authority to the PIPC to (i) recommend improvements of policies and systems, (ii) inspect whether the

[38] For historical background, see 'Personal Information Protection Commission' (KoreanLII undated) <http://koreanlii.or.kr/w/index.php?title=PIPC>.

recommendations are being implemented properly, (iii) request the submission of materials[39] and (iv) appoint or commission mediators to the Personal Information Dispute Mediation Committee.[40] The PIPC is now allowed to directly handle matters that are necessary for settling disputes.[41] PIPA was previously very non-specific about the PIPC's powers to intervene in disputes. PIPC still does not have power to issue compliance order or issue administrative fines. In relation to disputes, its role is to investigate, make recommendations, and when appropriate refer matters for mediation or for prosecution.

Amendments to the Network Act, and role of KCC

The Network Act regulates information and communication service providers (ICSPs), which includes a large range of the most important private sector information businesses. The continuing amendments to the Network Act (including to make some of its provisions match those of PIPA) demonstrate that it remains as important as PIPA, and the Korean Communications Commission (KCC) continues to be a key regulatory body concerning privacy issues.

Whon-il Park '[Recent amendments to the Network Act](http://koreanlii.or.kr/w/index.php/Recent_amendments_to_the_Network_Act)' (on KoreanLII)[42] – Park notes among the most important 2016 changes:

- If personal information is leaked via networks, KCC or KISA may demand that the ICSP concerned should delete or block the relevant information, subject to a penalty for negligence up to 30 million won;
- ICSP shall notify data breaches to the affected user where a user has collected personal data of others or caused others to provide personal data in a fraudulent manner via networks;.
- ICSPs responsible for provision of personal data to foreign countries without the consent of users shall be subject to the penalty surcharge up to 3% of sales related to such violation (see above comments on data export restrictions);
- KCC may recommend disciplinary action for violations against ICSP management.

Park notes among the 2015 amendments that personal information of users who do not use an ICSP's services shall be destroyed within one year unless otherwise provided by other laws or at user request.

Stronger enforcement laws and penalties

There have been numerous changes to enforcement provisions in Korea's data privacy laws since 2014, only some of the most important of which are mentioned here.[43]

---

39 PIPA (Korea), arts. 8, 11(1) and 63(4).

40 PIPA (Korea), arts. 40(3) and (4).

41 PIPA (Korea), art. 40(8).

42 http://koreanlii.or.kr/w/index.php/Recent_amendments_to_the_Network_Act

43 For details of many of the changes summarised in the following, see Kwang-Bae Park and Hwan-Kyoung Ko, 'Amendments to the Credit Information Act Promulgated on March 11, 2015', Lee & Ko Data Protection / Privacy Newsletter, March 2015 <http://www.leeko.com/newsl/dpp/201503/dpp1503_eng01.html>;Kwang-Bae Park and Hwan-Kyoung Ko, "Amendment to the Personal Information Protection Act Passed in the National Assembly on July 6, 2015 - Adoption of punitive damages, statutory damages provisions", Lee & Ko Data Protection / Privacy Newsletter, July 2015. <http://www.leeko.com/newsl/dpp/201507/dpp1507_eng1.html>; Kwang-Bae Park and Hwan-Kyoung Ko, "MOGAHA Announces Updated 'Standards of Personal Information Security Measures'" Lee & Ko Data Protection / Privacy Newsletter, February 2015.

Punitive and statutory damages Problems caused by difficulties of obtaining proof of damage for consumers in civil damages actions following massive data spills have now been addressed by reforms to the Network Act, the Credit Information Act, and to PIPA.

Amendments to the Network Act in May 2014 provide that ICSPs may be required by a court to pay statutory damages of up to KRW 3 million (around US$3,000) to each affected user for a negligent or wilful violation of a data protection requirement that causes data loss, theft, or leakage, without the user having to prove actual damage resulting from such violation. Amendments to the Credit Information Act in March 2015 provide, where there is wilful misconduct or negligence by the relevant business, (i) for punitive damages of up to three times the damage caused by personal credit information being lost, stolen, leaked, fabricated, or damaged; and (ii) for statutory damages of up to KRW3 million (around US$3,000) per data subject whose personal credit information was stolen, lost, leaked, fabricated, or damaged due to the. Amendments to PIPA in 2015 (effective 25 July 2016) provide for both punitive damages and statutory damages. A court may now order a data processor to pay an amount up to three times the actual damages of the data subject ('treble damages') if the data subject can prove: (i) an intentional or grossly-negligent violation of the PIPA by the handler; (ii) that the data subject's personal information was lost, stolen, leaked, forged, falsified or damaged due to such violation; and (iii) the actual amount of damages resulting from such a violation.[44] The PIPA amendment also added a statutory damages provision that allows a data subject to claim up to KRW 3 million (around US$3,000) in damages when the data subject can prove (i) wilful misconduct or negligence of the handler, and (ii) the fact that data subject's personal information was lost, stolen, leaked, forged, falsified or damaged because of the wilful misconduct or negligence.[45] Like the statutory damage provisions under the previously amended Network Act and Credit Information Act, this new statutory damage provision under the PIPA applies even if the data subject is unable to prove the actual amount of damage caused by the violation of the PIPA by the data processor.

Administrative surcharges based on turnover Following amendments to the Network Act in May 2014, ICSPs may be required by KCC to pay increased administrative fines of up to 3% (previously 1%) of the ICSP's annual turnover for failure to obtain user consent prior to the collection and use of personal information, and the cap of KRW 100 million (around US$100,000) for administrative fines previously applicable to data leaks resulting from failure to comply with technical and managerial protection measures was removed.

The first application of these major penalties was in relation to the 'Interpark data leak'[46] which resulted in KCC imposing an administrative surcharge of 4.5 billion won (around US$4.5 million) on one of the largest Korean online shopping malls. Cyber criminals, allegedly associated with North Korea, fraudulently obtained personal information of 10.3 million customers, and attempted to blackmail the company for KRW 3 billion (around US$3 million). The fine was imposed for negligent failure to protect customer data, and was 60 times higher than previous fines.

Amendments to the Credit Information Act in March 2015 similarly provided for administrative penalties of up to 3% of the annual revenue of a business for disclosure for non-business purposes of confidential data, or knowing use of illegally disclosed data and

---

44 PIPA (Korea), art. 39(3); Network Act, art. 32(2).

45 PIPA (Korea), art. 39-2; Network Act, art. 32-2.

46 Whon-il Park 'Interpark data leak' (KoreanLII, 2017) < http://koreanlii.or.kr/w/index.php/Interpark_data_leak>.

up to KRW5 billion (US$5 million) where failure to establish a security plan results in personal credit information being lost, stolen, leaked, fabricated, or damaged.

Other changes to PIPA penalties Amendments allowing fines proportional to turnover have not yet been made to PIPA. However, PIPA's 2015 amendments provided that a person who falsely or by other fraudulent means or methods acquires personal information processed by another person and then provides such personal information to a third party for profit-seeking or other illegitimate purpose will be subject to imprisonment of up to 10 years or a fine of up to KRW100 million (around US$100,000).[47] Also any person who suspends, interrupts or disrupts the operations of the public institutions by altering or deleting personal information processed by them shall be subject to the same punishment.[48] If personal information is stolen, lost, leaked, falsified, fabricated, or damaged because the data processor failed to implement the necessary security measures for the protection of personal information, then he/she will be subject to a fine of up to KRW20 million (around US$20,000) (double the previous maximum).[49] Any criminal proceeds that a person acquires from the illegal distribution or the like of personal information may be confiscated or collected by the courts.[50]

Cloud computing law

The most recent addition to Korea's suite of data protection laws is the Act on the Development of Cloud Computing and Protection of its Users (the " Cloud Computing Act"), which came into effect in September 2015, six months after promulgation. The Cloud Computing Act was designed to provide a framework for promoting the use of cloud computing while also aiming to protect the user data of such cloud services. Companies that use cloud services provided by another company are eligible to obtain business licenses and permits required under other laws, because they will be deemed to be equipped with the computing facilities stipulated by such laws, even if they do not have their own computing facilities.[51] However, this provision will not apply in certain cases, such as where the subject law prohibits the use of cloud computing. The Cloud Computing Act also stipulates that, fundamentally, the PIPA and Network Act will apply to the protection of user data stored on clouds ('Cloud Data') but it also includes separate provisions on the protection of such Cloud Data.[52] Specifically, cloud computing service providers ('CCSPs') are required to notify users of any cyber security incidents, data leakages, and service interruptions, and also notify the Minister of Science, ICT & Future Planning ('Minister of SIP') in the event Cloud Data is leaked.[53] Users may also demand from the CCSP the names of any countries in which their Cloud Data is stored, and, if the Minister of SIP determines that such disclosure is necessary for user protection, he may recommend that the CCSP provide the said country information to its users.[54] Finally, the provision of Cloud Data to third parties by CCSPs is also strictly limited, and, upon expiration of the service agreement between the CCSP and the user or the termination of cloud services, the

---

47 PIPA (Korea), art. 70(2).

48 PIPA (Korea), art. 70(1).

49 PIPA (Korea), art. 73(1).

50 PIPA (Korea), art. 74-2.

51 Cloud Computing Act (Korea), art. 21.

52 Cloud Computing Act (Korea), art. 4.

53 Cloud Computing Act (Korea), art. 25.

54 Cloud Computing Act (Korea), art. 26

CCSP is obligated to return the user's Cloud Data to the user or destroy such data if returning it is impossible.[55]

6. Taiwan—A Stronger Law, on a Constitutional Base

Taiwan continues not to have any specialised data protection authority. Taiwan has stated that it 'hopes to participate' in APEC CBPRs.[56]

Principles

Chen Hui-ling 'Taiwan and the right to be forgotten' (2015/05/04, Winkler Partners website)[57] - *Shi v. Google International LLC (Taiwan)*, a case of first impression involving the right to be forgotten recently came before the Taipei District Court. Despite an inconclusive District Court decision, Taiwan's history of adopting European data protection standards and shifting public opinion in Taiwan suggest that the right to be forgotten could be created in the future.

Chen Hui-ling and Michael R. Fahey 'Amendments to Taiwan data protection law take effect' (Winkler Partners website, 2016/04/06)[58] - Amendments to Articles 6-8, 11, 15, 16, 19, 20, 41, 45, 53, and 54 of Taiwan's Personal Information Protection Act (PIPA) took force on 15 March 2016. The most important change is that Taiwan now has enhanced protection for special categories of sensitive data. At the same time, compliance with Taiwan's data protection rules has been made easier by relaxing the consent requirement for ordinary personal data and reducing the risk of criminal liability for violations of the PIPA.

Enforcement

Chen Hui-ling and Michael R. Fahey 'Data protection enforcement decisions by Taiwan's Financial Supervisory Commission' (Winkler Partners website, April 2017).[59] - The only regulator that publishes its data protection enforcement decisions is the Financial Supervisory Commission ("FSC"). The FSC is Taiwan's super-regulator for financial industries. In this role, it oversees securities and futures firms, banks, and insurers. FSC data protection enforcement decisions are thus an important source for understanding enforcement of the PIPA by Taiwan's executive branch.

7. China—From Warring States to Convergence?

Since 2014 there has been substantial strengthening of various aspects of China's data privacy laws, in criminal law, tort liability, and data exports/data localisation. As discussed below, the Cybersecurity Law's provisions relating to data privacy articulate what are China's most comprehensive and broadly applicable set of data privacy principles to date, but they still fall slightly short of constituting a data privacy law meeting minimum international standards. They must also be read in the context of China's expanding data surveillance systems.

Data surveillance context

During the Xi Jinping administration (from 2012) there has been a move away from the previous two decades' growing emphasis on the rule of law, toward a more political emphasis

---

[55] Cloud Computing Act (Korea), art. 27.

[56] Taiwan Executive Yuan Taiwan's achievements during 2016 APEC Economic Leaders' Week', 8 December 2016 <http://english.ey.gov.tw/News_Hot_Topic.aspx?n=9CAC6D643D2B87F8&sms=C7706D6F9D246174>

[57] http://www.winklerpartners.com/?p=6198

[58] http://www.winklerpartners.com/?p=7167

[59] http://www.winklerpartners.com/?p=7808

on party-state control in China. One aspect of this is the rapidly growing development of an extensive data surveillance system combining information from both the public and private sectors, the Social Credit System (SCS) utilising 'big data' techniques, and intended to be widely accessible to many organisations, both public sector and (in some cases) private sector. The blueprint for the SCS is a State Council Guiding Opinion of May 2016.[60]

The most detailed explanation of China's emerging SCS, and its relationship to data privacy laws and principles, is Chen and Cheung's 2017 article 'The Transparent Self Under Big Data Profiling'.[61] They explain that implementation to date has primarily been through pilot legislation implemented at the local level in various parts of China since 2014. The concept of 'social credit' has been expanding to encompass many different indicia of 'trustworthiness' and is used for many different types of decisions. It is involving the combination of data from many different government sources, with a range of private sector sources, including financial information and information from social media – but to a still uncertain extent. Legislative control, particularly from a privacy perspective, of the various SCS implementations varies considerably between regions, and does not cover most basic principles of data privacy laws (though it often does cover some). The complexity of the SCS cannot be summarised here.

The developments outlined in the articles and discussion following are largely to do with China's private sector, and have only limited application to the public sector, whereas the SCS is primarily regulated (if at all) by public sector laws.

Criminal law

S. Livingston, and G. Greenleaf, China Whys and Wherefores – Illegal Provision and Obtaining of Personal Information Under Chinese Law (2014) 131 Privacy Laws & Business International Report 1-5.[62] In August 2014, Briton Peter Humphrey and his wife, naturalized American citizen Yu Yingzeng, were convicted by a Chinese court for violating the PRC Criminal Law's prohibition on illegally obtaining the personal information of others, and given prison sentences. This article considers how China's Criminal Law personal information protection provision, Article 253(a), has been interpreted since its introduction in 2009, beginning with a brief account of the history of the Humphrey case, followed by an examination of Article 253(a) and its subsequent interpretation in the Humphrey and other cases. The article considers issues such as the scope of Article 253(a) in relation to industries covered, in light of twenty reported cases involving illegal sale of personal data, and two cases of illegal 'obtainment', and what is a 'serious violation' (including the relevance of political factors). Examples from the large number of other cases based on the same article are given. Finally, the implications of the Humphrey case for foreign businesses in China are considered.

Tort liability

Livingston, Scott and Greenleaf, Graham, The Emergence of Tort Liability for Online Privacy Violations in China (2015) 135 Privacy Laws & Business International Report 22-24.[63] Between 2009 and 2014, China's legislative organs promulgated a series of fundamental data

---

[60] State Council (China) 'Guiding Opinions concerning Establishing and Perfecting Incentives for Promise-keeping and Joint Punishment Systems for Trust-Breaking, and Accelerating the Construction of Social Sincerity' *China Copyright and Media*, translated by Rogier Creemers, 30 May 2016, updated 18 October 2016, <https://chinacopyrightandmedia.wordpress.com/2016/05/30/state-council-guiding-opinions-concerning-establishing-and-perfecting-incentives-for-promise-keeping-and-joint-punishment-systems-for-trust-breaking-and-accelerating-the-construction-of-social-sincer/>.

[61] Y. Chen and A. Cheung 'The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System' , 27 June 2017, SSRN working paper < https://papers.ssrn.com/abstract=2992537>

[62] https://ssrn.com/abstract=2541570

[63] https://ssrn.com/abstract=2636129

privacy laws and regulations. Amongst these developments is an increased attention to providing individuals a civil recourse (or tort action) in instances where their personal privacy has been violated by online activities. This article focuses on such protections as existed via China's 1986 General Principles of the Civil Law (GPCL), and their subsequent codification in the 2009 Tort Liability Law (TLL). However, these developments have not, in themselves, led to a significant level of litigation, possibly due to uncertainly over how the TLL would function in this area. However some cases under the GPCL, notably the *Wang Fei* case, may have a continuing significance for the meaning of privacy under Chinese law, and on the role of intermediaries (IISPs).

S. Livingston, and G. Greenleaf, Tort Liability for Online Privacy Violations in China: The 2014 SPC Regulation (2015) 136 Privacy Laws & Business International Report, 24-27.[64] China's Tort Liability Law (TLL) includes two articles protecting an individual's right to privacy. Article 2 provides a civil right of action for violation of an individual's "right to privacy" among other "civil rights and interests." Article 36 specifically protects these civil rights and interests from online infringement. Yet there have been few reported cases to date, possibly because Chinese courts may not have understood how to apply Article 36 to privacy matters, and so may have been unwilling to accept such cases. In a bid to clarify, China's Supreme People's Court passed a regulation in October 2014 entitled "The Supreme People's Court Regulations Concerning Some Questions of Applicable Law in Handling Civil Dispute Cases Involving the Use of Information Networks to Harm Personal Rights and Interests." (SPC Regulation). It clarifies procedural questions relating to Article 36 while also taking the opportunity to add several new substantive provisions. This article analyses both the procedural and substantive aspects, and concludes that the SPC Regulation has the potential to place civil actions far more in the centre of the resolution of privacy disputes in China. It gives explicit guidance on many key points to all of China's courts in how to deal with such cases, which will both encourage potential litigants and their lawyers to commence cases, and encourage the courts to deal with them. A specific reference to compensation up to US$80,000 may assist.

Data localisation and data exports

S. Livingston and G Greenleaf, Data Localisation in China and Other APEC Jurisdictions (2016) 143 Privacy Laws & Business International Report, 22-26[65] Data localisation provisions are becoming commonplace around the world, not just in Russia. In many of these countries, local data protection laws may require that certain categories of data must be stored and processed on local servers within the country. Such provisions may require that some or all categories of personal data may only be stored and processed on local servers, or they make their export subject to conditions. Both types of provision may be called 'data localisation'. Such laws are controversial. The focus of this article is the data localisation requirements which are now emerging in China, an APEC member even though it has not proposed to become a party to the TPP. As yet, China's data localisation laws are only sectoral. Another version may soon be enacted in the Cybersecurity Law (nearing finalisation), which requires that "critical information infrastructure" ("CII") providers to store "citizens' personal information and important business data" within China unless their business requirements necessitate overseas storage and they have passed a security assessment regarding such storage and transfer. Such a provision will have significant implications for many foreign businesses operating in China.

---

[64] https://ssrn.com/abstract=2677533

[65] https://ssrn.com/abstract=2895610

Greenleaf, Graham and Livingston, Scott, China's New Cybersecurity Law – Also a Data Privacy Law? (December 1, 2016). (2016) 144 Privacy Laws & Business International Report 1-7.[66] In November 2016, China's Standing Committee of the National People's Congress (SC-NPC) promulgated the PRC Cybersecurity Law, which will take effect on 1 June 2017. The law is mainly devoted to provisions concerning the security of information networks and, in particular, to mandating security procedures and requirements for 'critical information infrastructure' and 'critical information infrastructure operators'.

However, the Cybersecurity Law's provisions relating to data privacy articulate what are China's most comprehensive and broadly applicable set of data privacy principles to date. These data privacy provisions reiterate many of the basic principles and requirements found in other laws and regulations, but the Law also includes new or more explicit requirements with respect to data correction rights, deletion, re-use and disclosure, breach notification to users and data localization. Still missing, however, are several common elements of other jurisdictions' data privacy laws, such as explicit user access rights, requirements on data quality and special provisions for sensitive data. The Law does not establish a national data protection authority. There are also uncertain questions of scope, particularly in relation to public sector bodies. While China has long lacked a broadly applicable national data privacy law, the scope and strengthened principles of this new legislation means that it can probably now be considered to be "China's Data Privacy Law," with which other lower-level laws and regulations must be consistent. This article analyses the privacy-related aspects of the Cybersecurity Law, and in particular asks what (if anything) it adds to China's previous set of data privacy laws. Comparisons are made with China's previously existing data privacy laws.

2017 Chinese developments: Extracts adapted from S. Livingston and G Greenleaf PRC's new data export rules: 'Adequacy with Chinese characteristics'? (2017) 147 *Privacy Laws & Business International Report* – China has introduced a draft piece of legislation, the *Measures for the Security Assessment of Personal Information and Critical Data Leaving the Country (Draft for Public Comment)* ('Draft Security Measures'), that sets its own limits on data exports by covered parties. This legislation is intended as an implementing regulation for the recently released *PRC Cybersecurity Law* ("Cybersecurity Law"), which also contains a data localization provision requiring certain "Key Information Infrastructure Operators" ("KIIOs")[67] to store on PRC servers all personal and "important" data collected through their China operations.

Data localization requirements – China's data localization requirements were made official in November 7, 2016 with the official promulgation of the *PRC Cybersecurity Law* by the Standing Committee of the National People's Congress. The law took effect on June 1, 2017. Article 37 of the Cybersecurity Law requires KIIOs to store on local servers all personal information and "important data" collected or processed through their operations in China.[68] This data may not be transferred overseas unless such transfer is necessary for a "critical business purpose" and only following a government-defined security review. Which entities are KIIOs remains vague (see previous article), and this attracted criticism. This criticism was heightened following the April 2017 public release of the first version of the Draft Security Measures, which contained language expanding these data localization requirements to cover "network operators", another ill-defined and possibly broad reaching category. Perhaps in

[66] https://ssrn.com/abstract=2958658

[67] These KIIO are sometimes referred to as "Critical Information infrastructure Operators" depending on how the first term (*guanjian)* is translated.

[68] Under a set of draft standards released on May 27, 2017, "important data" is defined as "Data that has a close relation with national security, economic development, and the public interest." This definition is then clarified through an extensive listing of potential important data in various sectors. See *Information Security Guidelines – Guidelines for Data Cross-Border Transfer Security Assessment (Draft)*. <http://www.tc260.org.cn/ueditor/jsp/upload/20170527/87491495878030102.pdf>.

response to these concerns, a second version of the Draft Security Measures was privately circulated in May 2017, which dropped the controversial data localization expansion and gave network operators until December 31, 2018 to comply with the data export provisions.[69] It remains unclear if these provisions will be included in the final draft. Although the Draft Security Measures, along with several other implementing regulations, were meant to have been made effective concurrent with the Cybersecurity Law on June 1, they have yet to be officially promulgated, nor is there any indication that a final version is imminent. The Cyberspace Administration of China (CAC) has only said that implementation regulations will be brought in within a year of the law's commencement, but in the interim companies should observe the Cybersecurity Law.[70] The May draft is at present the only indication of what the final Measures may contain, but it appears that these items are still being negotiated by industry stakeholders both foreign and domestic.

Data export requirements – The Draft Security Measures are principally important for how they affect the cross-border data export of 'network operators' in China. Under Article 2, the proposed measures would apply to all network operators seeking to export overseas personal information and "important data" collected and generated in the course of their operations within China. "Network operators" are defined in Article 15 as referring to "network owners, administrators, and network service providers", the same definition as in Article 76(3) of the Cybersecurity Law. The included term "network service providers" is not clearly defined under Chinese law and could be read broadly to encompass not only technology/online companies but also any company that uses its own IT networks or infrastructure. In the previous (April) draft, the security reviews also appear to be extended by what was then Article 16 to apply to all 'other individuals or organizations that collect and process personal information and important/critical business data within the borders of the PRC'. This incredibly broad expansion has been removed from the May draft.

In most cases network operators are permitted to self-assess the cross-border transfer based on the 'type, volume and sensitivity' of the data (Article 6). Network operators are then instructed to reassess the security of the transfer whenever there is a "substantial change in the purpose, scope, type or volume of the cross-border transfer of data, or where there the data recipient is changed or has experienced a significant security incident."

In any of the above circumstances, the network operator is required to submit a report to the relevant industry regulator, and then entrust them to conduct a security review, if any of three defined situations apply:

- The data aggregates or contains the personal information of more than 500,000 individuals;[71]
- The data contains information on certain matters related to national security (e.g., nuclear facilities, population and health records or megaproject activities) or cybersecurity-related information such as security vulnerabilities or specific security measures of key information infrastructure;
- 'Other information likely to affect national security and societal and public interests'.

[69] All quotations in this article refer to the May version of the Draft Security Measures, unless referred to otherwise.

[70] Teh, K and Kwok, P 'The Cyberspace Administration of China Clarifies the Cybersecurity Law' Dechert LLP, 1 June 2017 <https://info.dechert.com/10/8780/june-2017/the-cyberspace-administration-of-china-clarifies-the-cybersecurity-law.asp?sid=a37fd2ea-fea1-4a8f-a452-ad328dab2d68>

[71] The April 2017 draft of the Draft Security Measures included an additional category in instances where the volume of the data exceeded 1,000 GB. This was removed in the May 2017 draft.

The draft's reliance on individual industry regulators to carry out the security assessments raises a fear that these security reviews may be applied unevenly across industries, thus potentially posing further hurdles for companies whose products or services straddle different sectors.

Factors involved in a security assessment – Article 8 of the Draft Security Measures provides that a security assessment of a cross-border transfer of data (by either a network operator or an industry regulator) should focus on the following matters:

(1) the legitimacy, propriety and necessity for the cross-border transfer;
(2) the personal information involved, including the volume, scope, type, and sensitivity of the data, and whether the data subject has consented;
(3) the important data involved, including its volume, scope and type;
(4) the security protection capabilities of and measures taken by the data recipient, and the environment of the nation and region where the data recipient is located;
(5) the levels of risks of data being leaked, damaged, tampered with, or misused after the cross-border transfer or subsequent retransfer;
(6) the risks to nationals security, social and public interest, as well as lawful interests of individuals.

Mandatory blocking of some overseas transfers – Article 9 of the Draft Security Measures sets out five conditions that would prohibit the transfer of data outside of China:

1) The cross-border transfer is in violation of relevant laws, regulations or rules;
2) The data subject has not consented to the cross-border transfer of the information;
3) The cross-border transfer will damage public and national interests;
4) The cross-border transfer will endanger the security of [any of a very wide range of national security interests]; or
5) Other situations where the CAC, Ministry of Public Security and Ministry of State Security have determined that no overseas transfer shall take place.

In these situations, there is effectively mandatory data localisation: the data must stay in China. Each of these conditions, other than data subject consent, involves some element of discretionary decision-making, because these determinations are made by each industry regulator, with the overall guidance of the CAC (Art. 5).

Article 4 of the Draft Security Measures reiterates the need to adequately inform and obtain the consent of the data subject regarding the 'purpose, scope and type' of any overseas transfer, and the country or region where that recipient is located. The first (April) draft also required that the data subject be informed of the content or the transfer and the identity of the recipient. The notice obligations have therefore been reduced substantially. Consent from the data subject will be deemed to have been obtained where it results from the 'active behaviour' of the data subject, such as international phone calls or instant messaging, or cross-border Internet trading. Consent is not required in 'urgent circumstances under which the security of citizens' lives or properties are endangered'.

Other developments

Other 2017 Chinese developments: The Chinese government's growing recognition of an individual's right to privacy, is demonstrated most recently by its identification of the "right to privacy" as a specific individual right in the latest version of the *General Provisions of the Civil Law* promulgated by the National People's Conference on March 15, 2017.

The Draft Security Measures should also be viewed in tandem with the recently promulgated *Interim Security Review Measures for Network Products and Services*, which requires a security review of certain imported foreign IT equipment and services to ensure they are 'secure and controllable.' Under this separate measure, inbound IT equipment and services are to be assessed for various risks, among which is the risk the products or servers will be illegally controlled, interfered with, or interrupted or that the provider of the product or service may use it to illegally collect, store, process or use its users' personal information.

8. Japan—The Illusion of Protection

Japan's law has undergone major changes since 2014, but the 2015 amendments to Japan's Personal Information Protection Act (PIPA) only came into effect on 30 May 2017.

Intentional engagement

Japan is now a full participant in APEC's CBPRs (see Chapter 2 update 'Japan Joins APEC-CBPRs: Does It Matter?'), and is also an observer on the Convention 108 Consultative Committee.

Japan is also seeking a positive adequacy assessment from the EU. On 4 July 2017 the European Commission and Japan issued a joint statement[72] which 'acknowledged that the recent reforms of their respective privacy legislation have further increased the convergence between their two systems', and referred to the possibility of 'simultaneous finding of an adequate level of protection by both sides' (Japan's revised law allows the possibility of such 'white-list' findings), and the objective of 'achieving this goal by early 2018, including by addressing relevant differences'. This commitment comes at the same time as the EU is advancing a free trade agreement (FTA) with Japan,[73] but the decision on adequacy is proceeding under a separate process, as required by EU law.

Principles and enforcement

G. Greenleaf, Japan: Toward International Standards – Except for 'Big Data' (June 19, 2015). (2015) 135 Privacy Laws & Business International Report, 12-14.[74] – The Abe Government introduced into Japan's Diet in March 2015 a Bill for the first significant changes to its data privacy law of 2003, the Personal Information Protection Act (PIPA). The Bill's reforms which will bring Japan's closer to international standards for privacy principles, plus a new data protection authority which has significant powers, and requirements to act independently. It is a Bill significantly stronger than was indicated by early drafts. The Bill was passed unchanged by the lower House of Japan's Diet in May 2015. This article analyses the Bill's proposals, and reaches some conclusions about what will be needed to make them effective. The Bill will create for the first time in Japan a data protection authority (DPA), the Personal Information Protection Commission (PIPC), which will have jurisdiction in relation to the whole private sector, although not the public sector. The extent of likely independence of the PIPC, and the strength of its powers, are assessed.

Japan's current law [prior to these amendments had] the weakest privacy principles of any Asia-Pacific country that has a data privacy law. This Bill takes substantial steps to address such criticisms, and it is shown that these changes, once enacted, will bring the principles in

---

[72] European Commission 'Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan on the state of play of the dialogue on data protection', 4 July 2017 <http://europa.eu/rapid/press-release_STATEMENT-17-1880_en.htm>

[73] D. Vincent 'EU-Japan one step closer to signing trade deal, Euractive , 4 Jauly 2017 <http://www.euractiv.com/section/economy-jobs/news/eu-japan-one-step-closer-to-signing-trade-deal/>

[74] https://ssrn.com/abstract=2649556

Japan's law to a similar position to most other Asian or Asia-Pacific countries with data privacy laws: stronger than the basic OECD principles, and about mid-way toward the 'European' principles of the EU Directive or the Council of Europe Convention.

The overall conclusion is that the effectiveness of the new Act is going to depend a great deal on the chairperson and members of the PIPC, because so much of the content of the legislation will now be found in delegated legislation made by the PIPC.

'Big data' / 'anonymised data' provisions

G. Greenleaf, Japan: Toward International Standards – Except for 'Big Data' (June 19, 2015). (2015) 135 Privacy Laws & Business International Report, 12-14.[75] – 'Big data' provisions concerning use of 'anonymised' data are still included [in the revised Bill], but there are significant controls on business use of such data. The new concept of 'anonymous process information' (API) is explained. Although API is not 'personal information', many protective provisions similar to those applied to personal information apply to API. Businesses will therefore need to consider carefully the business case for the creation or use of API, given these obligations.

9. Macau SAR—The 'Euro Model'

Macau's Office for Personal Data Protection (GPDP) still has not been formally established by its own legislation, but continues to operate as a 'project' under the Chief Executive's Office, twelve years after the PDPA was enacted. Yang Chongwei (Ken Yang) was sworn in on 4 July 2017 as the new co-ordinator of the office,[76] have served as deputy since its inception.

The GPDP continues to have what is arguable the most transparent practice in Asia concerning publication of its enforcement activities. In each of 2015 and 2016 it published 20 case notes concerning complaint resolutions[77] (in English translations, even though English is not an official language in Macau), as well as the occasional authorisation of data exports.[78]

10. Singapore—Uncertain Scope, Strong Powers

The PDPC has issued an update to Chapter 3 'Anonymisation' to its Advisory Guidelines.[79] Since the Guidelines use 'anonymisation' to refer to de-identification processes which 'can be reversible or irreversible' they must be read with considerable care, because, as the Guidelines say with considerable understatement 'reversibility of the specific process used would be a relevant consideration … when managing the risk of re-identification.'[80]

PDPC Commissioner Tan Kiat How has mentioned that PDPC would start setting up a TrustMark for data privacy in Singapore in 2017, and that they were 'seriously looking into' joining the APEC-CBPRs.[81]

---

[75] https://ssrn.com/abstract=2649556

[76] R. Marques 'New privacy watchdog intends to follow predecessors' steps', *Macau Times*, 5 July 2017

[77] OPDP (Macau) 'Complaint Case Notes' <http://www.gpdp.gov.mo/index.php?m=content&c=index&a=lists&catid=209>.

[78] OPDP (Macau) 'Authorisations' <http://www.gpdp.gov.mo/index.php?m=content&c=index&a=lists&catid=206>.

[79] PDPC (Singapore) *Advisory Guidelines on the PDPA for Selected Topics,* revised 28 March 2017 <https://www.pdpc.gov.sg/docs/default-source/advisory-guidelines---selected-topics/ch-3---anonymisation-(20170328).pdf?sfvrsn=2>

[80] PDPC (Singapore) *Advisory Guidelines*, [3.1].

[81] Tan Kiat How 'Breakfast with the Commissioner' presentation, Singapore Business Federation, Privacy Awareness Week 2017 <https://www.pdpc.gov.sg/news/Events/page/0/year/2017/month/All/breakfast-with-commissioner-(paw-2017>.

Data export provisions

G. Greenleaf, ASEAN Data Privacy Developments 2014-15 (2015) 134 PLBIR[82] - The Personal Data Protection Regulations 2014 (PDPR) were made on 15 May 2014. The most important aspects of the Regulations concern data exports, where Singapore takes a distinctive approach.

Enforcement

G. Greenleaf, Singapore Starts Privacy Enforcement: Fines for Lax Security (2016) 141 Privacy Laws & Business International Report, 1, 4-6.[83] Singapore's Personal Data Protection Commission (PDPC) has published nine data protection enforcement decisions, the first since the Personal Data Protection Act 2012 (PDPA) came into force in July 2014. It has also issued advisory guidelines on enforcement. This article outlines these developments and their significance. In the PDPC's most significant decision, fines of US$35,000 (S$50K) were ordered against K Box Entertainment Group and S$10K against its data intermediary, Finantech Holdings, primarily for breaches of the security principle. Other companies and voluntary associations were also fined. PDPC Advisory Guidelines on alternative dispute resolution make it clear that the PDPC will take an interventionist role to ensure that parties resolve disputes.

2016-17 Singapore developments: In April 2016 Singapore's Personal Data Protection Commission (PDPC) published its first nine enforcement decisions since its Act came into force in July 2014, and in little over a year has published details of 27 enforcement actions, including 22 in 2016.[84] The first case reported in April 2016 involved a US$35,000 (S$50,000) fine, [85] and while none have matched that, there has been one US$17,500 fine, and three US$7,000 (Singapore $10,000 fines), plus some lesser fines. About 75% of findings involve failures to provide reasonable security arrangements, and most of the others involved disclosures of personal information in breach of disclosure limitation obligations, which were not justified by consent or other defences. Security failures by data intermediaries occurred frequently. The data privacy principles in Singapore's Act are at the less onerous end of the spectrum,[86] but these cases make clear that there are many points where businesses cannot assume that the PDPC will adopt a broad and pro-business interpretation.[87]

11. Malaysia—ASEAN's First Data Privacy Law in Force

Enforcement

G. Greenleaf, Singapore Starts Privacy Enforcement: Fines for Lax Security (2016) 141 Privacy Laws & Business International Report, 1, 4-6.[88] In contrast, Malaysia's Department of Personal Data Protection has not yet shown any visible signs of enforcing its Personal Data Protection Act 2010, despite that Act being fully in force for over two years. One reason is that, in effect, the Malaysian PDPA can only be enforced through prosecutions, and those must be with the

---

[82] https://ssrn.com/abstract=2645702

[83] https://ssrn.com/abstract=2824783

[84] PIPC (Singapore) 'Data Protection Enforcement Cases' <https://www.pdpc.gov.sg/commissions-decisions/data-protection-enforcement-cases.>.

[85] G Greenleaf, Graham, Singapore Starts Privacy Enforcement: Fines for Lax Security (May 30, 2016). (2016) 141 Privacy Laws & Business International Report, 1, 4-6.

[86] G Greenleaf 'Singapore's Personal Data Protection Act 2012: Scope and Principles (with so Many Exemptions, it is only a 'Known Unknown') (2012) 120 Privacy Laws & Business International Report, pgs 1, 5-7.

[87] For a more detailed analysis see Ken Chia and Celeste Ang 'Data Privacy Enforcement Trends', 13 January 2017 <http://www.bakermckenzie.com/en/insight/publications/2017/01/data-privacy-enforcement-newsletter/>

[88] https://ssrn.com/abstract=2824783

consent of the Public Prosecutor. A new Regulation allows the Commissioner to offer to compound specified offences – in effect to allow a fine to be paid instead of prosecution.

2017 Malaysian developments: Since mid-2016, three Codes of Practice have been registered in Malaysia: PDP Code of Practice for Utilities Sector (Electricity); Code of Practice on PDP for the Insurance and Takaful[89] Industry in Malaysia; and PDP Code of Practice for the Banking and Financial Sector. Additional classes of data users required to register under the PDPA.[90]

Otherwise, apart from collecting registration fees, there is nothing on the PDPC website to indicate that the Commissioner has yet taken any steps to enforce the Act, such as reports of investigated complaints.

Ms. Khalidah Binti Mohd Darus has been appointed as the new Personal Data Protection Commissioner, effective January 23, 2017, succeeding Encik Mazmalek bin Mohamad who was Commissioner from October 2014. Puan Khalidah was the Deputy Director-General of the National Film Development Corporation Malaysia (FINAS).[91]

Data exports

Malaysia's Personal Data Protection Commissioner (PDPC) is perhaps the first in the world to publish a draft 'White List' of jurisdictions to which the Commissioner considers personal data may be transferred. Section 129(1) of the PDPA provides that: 'A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the Commissioner, by notification published in the Gazette.' Section 129(3) provides various exemptions, on which companies transferring data out of Malaysia may otherwise rely, and at present must rely in the absence of any s. 129(1) notifications. The Act does not set out criteria on which the Commissioner must base his decision.

The PDPC has published a Consultation Paper[92] which proposes policies which will guide it in making recommendations to the Minister under s129(1), together with a draft *Personal Data Protection (Transfer Of Personal Data To Places Outside Malaysia) Order 2017* ('Draft Order'). The PDPC refers to three criteria which it says it considered in drawing up its White List: (i) 'Places that have comprehensive data protection law (can be from a single comprehensive personal data protection legislation or otherwise a combination of several laws and regulations in that place)'; (ii) 'Places that have no comprehensive data protection law but are subjected to binding commitments (multilateral/bilateral agreements and others)'; and (iii) 'Places that have no data protection law but have a code of practice or national co-regulatory mechanisms'. Other than what can be implied from the words 'comprehensive data protection law' (which could just mean that it applies to all parts of the private sector), these criteria have no substance: the standard of data protection required is not stated, whether relative to the standard in Malaysia's law or any other standard.

Based on these rather slim criteria, the draft Order by the Minister simply lists the jurisdictions which the Commissioner would recommend that the Minister could declare. They are: (1) the EEA member countries (including EU countries); (2) the US; (3) countries

---

[89] A type of Islamic insurance, where members contribute money into a pooling system in order to guarantee each other against loss or damage.

[90] Personal Data Protection (Class of Data Users) (Amendment) Order 2016 (Malaysia).

[91] Christopher & Lee Ong law firm *Client Update*, February 2017.

[92] PDPC (Malaysia) *Personal Data Protection (Transfer Of Personal Data To Places Outside Malaysia) Order 2017*, Public Consultation Paper (PCP) No. 1/2017.

that have received positive EU 'adequacy' assessments; (4) Asian and Pacific regional countries with data privacy laws (Australia; Japan; Korea; China; Hong Kong; Taiwan; Singapore; and the Philippines); and (5) the Dubai International Financial Centre (DIFC). Macau is missing, surprisingly. This is not a politically courageous list. The US does not fit within any of the criteria supposedly applied. It is also questionable concerning China, given that the right of subject access is not yet clear in its laws, and there is uncertainty in the scope of China's various laws.[93] The other standard being applied here appears to be political expediency.

Some commentators have welcomed Malaysia taking this initiative: 'given that the growth of advanced, high tech economies in the region is likely to be aided by moves towards interoperability, Malaysia's open commentary on the adequacy of other data protection laws in the region is a welcome step forward'.[94] The problem is that this interoperability would be of the lowest common denominator (the US and China), and few other countries with data privacy laws are likely to agree.

12. The Philippines and Thailand—ASEAN's Incomplete Comprehensive Laws

The Philippines

G. Greenleaf, Philippines Appoints Privacy Commission in Time for Mass Electoral Data Hack (2016) 141 Privacy Laws & Business International Report, 22-23.[95] The Philippines Data Privacy Act 2012 (DP Act) was signed into law by President Benigno Aquino on 15 August 2012, and (in theory) came into effect 15 days after its publication (s. 45). The Act remained dormant, because until a National Privacy Commission (NPC) was appointed, and made Implementing Rules and Regulations (IRR), very few of its provisions were enforceable, and none were enforced. After nearly four years, the NPC has finally been appointed, and has taken up its role at a time of change of Presidents, combined with a massive data breach at the country's electoral commission (Comelec). Less than four months before the expiry of his Presidential term, Aquino finally appointed the three-person Commission, each for a three year term. Just after the NPC's appointment, the Commission on Elections (Comelec) website was hacked and defaced, and its database containing personal identifiable information of 55 million voters was copied and posted online. This article surveys this changed landscape, and the implications for businesses of the delayed coming into force of the Philippines' law. The NPC must make implementing rules and regulations (IRRs) within 90 days of its appointment, by early June 2016, and it will be another year before businesses and agencies must comply. The significance of the IRRs, the powers of the Commission, and the implications for businesses, are explained.

G. Greenleaf, Philippines Puts Key Privacy Rules in Place but NPC Faces Pressure (2016) 143 Privacy Laws & Business International Report, 19-21[96] The Philippines' new National Privacy Commission (NPC), only appointed in March 2016, by the predecessor to current President Duterte's, took swift steps to bring the Philippines Data Privacy Act (DP Act), dormant since enactment in 2012, into force.

---

[93] G Greenleaf, G and S Livingston 'China's Cybersecurity Law – also a data privacy law?' (2016) 144 *Privacy Laws & Business International Report*, 1-7

[94] Mark Parsons, 'Malaysia publishes draft "White List" for personal data exports' Hogan Lovells, Hong Kong, 27 April 2017 < https://www.hoganlovells.com/en/publications/malaysia-publishes-draft-white-list-for-personal-data-exports>.

[95] https://ssrn.com/abstract=2824419

[96] https://ssrn.com/abstract=2895600

On 25 August 2016 the NPC issued the finalized Implementing Rules and Regulations (IRRs) necessary for the Act to become effective. However, three days before the NPC issued the IRRs, Duterte purported to require the resignation of all its members. This article provides a brief account of the effect of the IRRs on the Data Privacy Act, the NPC's issuing of data breach notification rules (its other most significant action to date), and the implications of the attempted forced resignation of the Commission members.

It is arguable that the IRRs do add some substantive new obligations (but fewer or less onerously than the draft IRRs), in such areas as requirements for data sharing agreements to be approved by the NPC, and a right for data subjects to object or withhold consent to processing, particularly in relation to direct marketing, automated processing or profiling. The IRRs also add many other essential details as to how the Act will operate. Prior to issuing the IRRs, the NPC also issued a draft Rules of Procedure for Data Breach Notification and Other Responsibilities.

Businesses across the world are using the Philippines for outsourced data processing, and many may do so on the assumption that the Philippines has effective (or at least operative) data privacy laws, plus at least some adherence to the rule of law. All businesses using or considering data processing in the Philippines need to understand fully the contexts in which their work is being carried out, and consider the implications. Although their initial actions are commendable, the NPC's enforcement of the Act will need to be kept under close scrutiny until it becomes clear that the Philippines does in fact have a functioning Data Privacy Act.

2017 Philippines developments: The Philippines National Privacy Commission (NPC) has taken a very activist approach to carrying out its duties in its first year of operation. The most obvious indicator of this is that, following the massive data breach by the Commission on Elections (COMELEC) in March 2016, the NPC found[97] that the Commission on Elections (COMELEC) violated the Data Privacy Act and recommended the criminal prosecution of COMELEC Chairman J. Andres D. Bautista. No prosecution has yet commenced. One of the databases involved in the security breach contained sensitive personal data on over 75 million voters, a database on persons banned from holding firearms, with nearly 900,000 personal records, and another with data on 1,267 COMELEC employees, which the NPC describes as 'making the incident the worst recorded breach on a government-held personal database in the world, based on sheer volume.' The NPC alleges 'willful and intentional disregard of his duties as head of agency, … tantamount to gross negligence' by Bautista. Among numerous sections of the *Data Privacy Act* allegedly breached, s.26 penalizes accessing sensitive personal information due to negligence, imposes imprisonment from 3 to 6 years and a fine from US$10,000 to US$80,000 and exposes public officers to disqualification from public office for double the term of imprisonment.

The NPC also ordered that COMELEC must, within short time-frames, appoint a Data Protection Officer, conduct an agency-wide Privacy Impact Assessment and a Privacy Management Program and a Breach Management Procedure within three months, as well as observing the Implementing Rules and Regulations (IRRs) and Circular on Security of Personal Data in Government Agencies. The NPC has started investigating a second complaint against COMELEC, involving a data breach of a database held by a regional office concerning 55 million individuals. It has issued an interim compliance order[98] that COMELEC should erase all copies of this database in all offices, unless it can secure them appropriately, and that

[97] NPC Case No. 16-001 (Philippines), 28 December 2016; For a summary by the NPC, see < https://privacy.gov.ph/privacy-commission-finds-bautista-criminally-liable-for-comeleak-data-breach/>.

[98] Compliance Order dated February 13, 2017; see < https://privacy.gov.ph/npc-starts-probe-comelecs-2nd-large-scale-data-breach-issues-compliance-order/>.

all individuals affected by the breach must be notified, individually in one location, and by newspaper advertisements otherwise.

The NPC has not yet published results of any other investigations, so it is not yet known how its approach will translate into it dealings with private sector organisations, but these first complaints should help induce businesses to take the Act and the NPC seriously.

In May 2017 the NPC issued an advisory notice[99] setting out guidelines on the mandatory appointment of a data protection officer (DPO) by all personal information controllers (PICs) and personal information processors(s) in the Philippines, requiring immediate compliance.[100]

The NPC is engaging internationally, obtaining accreditations as a full member of the International Conference of Data Protection and Privacy Commissioners (ICDPPC), and as an observer to the Council of Europe Convention 108 Consultative Committee.

Thailand

G. Greenleaf, ASEAN Data Privacy Developments 2014-15 (2015) 134 PLBIR[101] - Thailand's military junta, the National Council for Peace and Order (NCPO), seized power from the elected Shinawatra government in early 2014, ending one of Thailand's longer periods of civilian and democratic government, since 2006. In January 2015, the junta's Cabinet approved a new *Personal Data Protection Bill* as part of a very controversial package of Bills. The Bill has not been enacted.

2017 Thai developments: Thailand, which was proceeding toward a law up to 2014, has been ruled by a military junta since mid-2014, with few privacy protections. [102] There is little sign of a draft *Personal Information Protection Act* being enacted, although it is being reviewed by numerous government and legislative bodies, [103] but there are quite a few sectoral regulations.[104]

13. Vietnam and Indonesia—ASEAN's Sectoral Laws

Vietnam

G. Greenleaf, ASEAN Data Privacy Developments 2014-15 (2015) 134 PLBIR[105] - Vietnam's laws dealing with data privacy were previously vague on the sanctions to be applied to breach of various principles, but this is no longer so. The government of Vietnam issued decrees effective January 2014 'providing guidance on sanctions for violations in the information technology and communications (ITC) sector,' implementing Vietnam's 2012 changes to its administrative sanctions regime.

---

[99] NPC Advisory No. 2017-01 (Philippines) on the *Designation of Data Protection Officers,* pursuant to Section 21(b) of the Data Privacy Act of 2012 (R.A. No. 10173) and Rule VI, Section 26(a) of its Implementing Rules and Regulations.

[100] Based on the NPC ruling that the period for complying with the Data Privacy Act of 2012 expired in 2013, one year after the effective date of the law. For Guidelines details, see Quisumbing Torres *Client Alert*, May 2017 <http://bakerxchange.com/rv/ff0030ab24dc859ce45b16c2c44c878fe158cc01/p=1116215>.

[101] https://ssrn.com/abstract=2645702

[102] Privacy International *State of Privacy – Thailand*, 14 March 2017 <https://www.privacyinternational.org/node/967>.

[103] DLA Piper *Data Protection Laws of the World – Thailand*, 24 January 2017.

[104] Tilieke and Gibbins 'Data security and cybercrime in Thailand', 8 February 2017, Lexology.

[105] https://ssrn.com/abstract=2645702

C. Schaefer and G. Greenleaf, Vietnam's Cyber-Security Law Strengthens Privacy… A Bit (2016) 141 Privacy Laws & Business International Report, 26-27.[106] Vietnam's new Law on Cyber-Information Security, which came into effect on 1 July 2016, is a law enacted by the National Assembly, so it is the second highest form of legislation in Vietnam. This article assesses whether the Law's scope, and the data privacy principles it sets out, significantly expand Vietnam's existing data privacy laws, which are scattered across various regulations that apply to the IT, telecommunications, banking, e-commerce and consumer privacy sectors. The Law provides clearer concepts of personal information and processing, but with a focus limited to commercial processing and only in cyberspace. The law is unusual in that it defines 'cyberspace' so as to suggests that the scope also includes VPNs and possibly certain intranets. Within this limited scope, the Law sets out what is probably the most comprehensive set of data privacy principles yet found in a Vietnamese law. However, it is unclear what the sanctions for the violations committed by organisations are under the Law until implementing regulations provide more details on consequences for violations by organisations.

S. Livingston and G Greenleaf, Data Localisation in China and Other APEC Jurisdictions (2016) 143 Privacy Laws & Business International Report, 22-26[107] Among APEC jurisdictions, China is not alone in adopting data localisation requirements. As well as the obvious example of Russia's very sweeping law, they are found in at least Indonesia and Vietnam in very general forms, and in Canada and Australia in sector-specific forms. These are also explained in this article.

2017 Vietnamese developments: Vietnam's Law on Cyber-Information Security, which came into effect on 1 July 2016, has probably the most comprehensive set of data privacy principles yet found in a Vietnamese law,[108] but still lacks regulations to clarify its enforcement. Amendments to the Penal Code were drafted, and planned to come into force at the same time, to impose specific 'criminal penalties for violations relating to cyber information and cybercrime' which previously had to be fitted under 'more traditional crimes, such as theft or fraud', but 'its implementation has been postponed indefinitely … due to the large number of errors discovered in the code'.[109]

Indonesia

Andin Aditya Rahman Indonesia to Introduce Personal Data Protection Rules in Electronic Systems (2016).[110] This Regulation is currently the most detailed data privacy law in force in Indonesia. This article gives a detailed analysis of this important regulation.

2017 Indonesian developments: Although Indonesia does now have a data privacy law meeting minimum international standards,[111] work continues on a more comprehensive law which includes, among other things, a data protection authority. A Draft *Bill on Personal Data Protection* was prepared in 2015 by the House of Representative, and the circulated by the Ministry of Law and Human Rights for discussion among all government institutions to ensure

---

[106] https://ssrn.com/abstract=2824405

[107] https://ssrn.com/abstract=2895610

[108] Christian Schaefer and Graham Greenleaf 'Vietnam's Cyber-Security Law Strengthens Privacy… A Bit' (2016) 141 *Privacy Laws & Business International Report*, 26-27 <https://ssrn.com/abstract=2824405>.

[109] Jim Dao, Tu Ngoc Trinh and Waewpen Piemwichai 'Data Security and Cybercrime in Vietnam' 8 February 2017, Tilleke & Gibbins <http://www.lexology.com/library/detail.aspx?g=37d6b3a7-f0aa-4a3f-8688-2e31967b1708>.

[110] https://andinadityarahman.com/indonesia-to-introduce-personal-data-protection-rules-in-electronic-systems/

[111] Andin Aditya Rahman 'Indonesia enacts Personal Data Regulation' (2017) 145 *Privacy Laws & Business International Report*, 1.

that there is no conflict between it and other sectoral rules. As a result of the plenary meeting of the Indonesian legislature held in early 2017, a new version of the Draft Bill ('2017 draft Bill') is available.[112] These processes are taking place earlier than observers had anticipated, considering that the Bill was not included in the House of Representative's priority list for new legislation.

Some features of this new draft include: its scope covers both Indonesian citizens and foreign citizens in Indonesia; there is comprehensive coverage of both private and public sectors, and some extra-territorial coverage; the principles included are extensive, including for example data breach notification to individuals; entitlement to claim compensation from a court for any infringements; and personal data transfers outside Indonesia based on both the consent of the data subject and the law recipient country providing 'an equal level of protection', or based on contract or international agreements, or an exemption from the Commission. An independent Commission is established to administer the law; to investigate and adjudicate on infringements; to conduct mediation between parties, with agreed results of mediation being enforceable; and to impose administrative penalty sanctions of at least US$75,000 (and up to 25 times as much).

14. Privacy in the Other Five Southeast Asian (ASEAN) States

There have been no significant privacy-related developments during in 2014-17 in the other four ASEAN states (Cambodia, Lao PDR, Myanmar) and candidate member Timor Leste.

Brunei

G. Greenleaf, ASEAN Data Privacy Developments 2014-15 (2015) 134 PLBIR[113] - The Brunei Government has adopted a Data Protection Policy which has applied since at least early 2014 to government Ministries and Departments, including educational institutions and statutory bodies (with numerous and ill-defined exemptions).

There are no other developments concerning Brunei.

Cambodia

There have been no developments concerning data protection or the right to information in Cambodia. The Hun Sen government remains in power.

Laos

There have been no developments concerning data protection or the right to information in the Lao PDR.

Myanmar/Burma

Although a 2015 parliamentary elections resulted in victory for the opposition National League for Democracy (NLD) and its leader Aung San Suu Kyi, the government is still dominated by the military. There has been no progress on a Right to Information law despite NGO campaigns, nor on data protection.

Timor Leste

A democratic election for a new President was held in 2017. Timor Leste's candidacy for ASEAN membership is not yet complete. There is no other update for this section.

---

[112] Rancangan Undang-Undang tentang Perlindungan Data Pribadi **(**2017 Indonesian draft Bill, in Bahasa – select '.docx') <http://www.peraturan.go.id/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html>

[113] https://ssrn.com/abstract=2645702

15. India—Confusion Raj, with Outsourcing

Development of data privacy in India is deadlocked until the Constitutional Court resolves the status of a right of privacy under India's constitution, and the effect of that decisions on the Aadhaar (ID system).

Privacy legislation and guidelines

India has done nothing to strengthen privacy protections since at least 2012, and what it had done by then (the IT Act s43A 'Rules') was derisory. India has twice been rebuffed by the EU in its attempts to obtain 'adequacy' status, and there are no reasons to expect that to change until it introduces a comprehensive data privacy law. There has been no visible progress on the draft The Right to Privacy Bill since 2014, but there are claims that the government will release a Bill during 2017.

Guidelines on the collection of identity information by government departments were issued in 2016 by the IT Ministry, under the *IT Act 2000* s43A and the *Aadhaar Act 2016*.[114] Since the previous s43A 'Rules' were limited in scope to 'bodies corporate', the application of even a set of non-enforceable Guidelines to the public sector is a step forward. These Guidelines may have some legal force under the Aadhaar Act 2016, but this is not clear.

ID system and constitutional right to privacy

In contrast to its inaction on a data privacy law, the Modi government, and many state governments and other institutions, are pushing relentlessly ahead to make India's ID system (the Aadhaar number) mandatory in all significant aspects of Indian life, and irrespective of any orders made by the Supreme Court.

G. Greenleaf, Confusion as Indian Supreme Court Compromises on Data Privacy and ID Number (2015) 137 Privacy Laws & Business International Report, 24-26, September 2015.[115] The fate of India's data privacy legislation and its ID system are intertwined, both depending on whether India's Supreme Court decides that India has an implied Constitutional right of privacy, and whether it extends to data privacy. In a decision in the *Puttaswamy Case* in August 2015 a three judge bench of India's Supreme Court (i) referred to a 'constitution bench' of at least five Justices the existence and content of the constitutional right of privacy; and (ii) in the interim, allowed India's 'Aadhaar' ID number system to continue operating, despite its alleged interference with privacy, but with limitations on how it may be employed. This article examines the Supreme Court's decision and the implications of both pro-privacy and anti-privacy constitutional findings for the future of the Aadhaar, and of comprehensive data privacy legislation for India. Since it is unknown how long it will take a constitution bench to be constituted or to reach a decision, the article concludes by explaining why (in the interim) India's current data privacy rules remain broken and ineffective. The article concludes that the Supreme Court's 'compromise' in *Puttaswamy* may turn out to be a capitulation. It may also result in continuing defiance or avoidance of Supreme Court orders by the Executive that is dangerous for India's constitutional relationships.

G. Greenleaf, Your Money or Your Life?: Modi's Deceptive Enactment of India's ID Legislation (2016) 140 Privacy Laws & Business International Report 18-20.[116] India's Modi government

---

[114] Ministry of Electronics and Information Technology 'General Guidelines for securing Identity information and Sensitive personal data or information in compliance to Aadhaar Act, 2016 and Information Technology Act, 2000' (undated, 2016?) <http://dgrpunjab.gov.in/Home/Download/5325>

[115] https://ssrn.com/abstract=2708954

[116] https://ssrn.com/abstract=2800835

inherited from its Congress government predecessors a national ID system, the Aadhaar, which has enrolled up to 800 million of India's 1.2 billion residents since 2009. Legislation to legitimise the system had been stalled in India's lower house (the Lok Sabha) since 2010, partly because of privacy concerns of legislators. Modi's government enthusiastically accepted this gift, promoting its expansion and defending it in the courts against constitutional claims that it infringed privacy. However, the Supreme Court still presented a potential legal road-block, with a case concerning the Aadhaar's constitutionality having been referred to a 'constitution bench' (to be appointed by the Chief Justice) for determination. Lack of a majority in the upper house (Rajya Sabha) presented a political obstacle to obtaining legislative legitimacy for the system, which still depended on a 2009 Executive decision for its imprimatur. This serial has had many episodes since 2009. This article explains how the Aadhaar legislation has unexpectedly been enacted, the basic structure of the ID system it establishes, its potential private sector uses, the privacy vacuum within which it will operate, and how it is now much more dangerous as a result of this enactment. A concluding question is whether this Bill is what Indians have been led to expect for the last seven years, or whether they have been deceived?

2016-17 Indian developments: In 2016 the 'Aadhaar Act', legislation to legitimate the Aadhaar and the entity operating it (the UIDAI) was finally enacted.[117] The UIDAI claims to have issued 112 crore (ie 1.2 billion) Aadhaar numbers so far, comprising 89.6% of India's eligible population, including an interesting 104% of those over 18 (as at 2015 population estimates).[118]

The UIDAI has made five sets of Regulations under the Aadhaar Act.[119] Their deficiencies have been analysed by the Center for Internet & Society (CIS), [120] including inadequate transparency in UIDAI meetings, un-addressed security issues, unclear and non-comprehensive grievance procedures, excessive storage of logs for seven years (but allowing individual access to those logs), and audits controlled by a non-existent certification body.

The government, which has effective Parliamentary majorities, in 2017 inserted s. 139AA in the *Income Tax Act*, so as to require mandatory linking of the Aadhaar number to a person's Permanent Account Number (PAN), a 10-digit alphanumeric number allocated by the Information Technology Department to individuals and entities. It provided in part '(1) Every person who is eligible to obtain Aadhaar number shall, on or after the 1st day of July, 2017, quote Aadhaar number– (i) in the application form for allotment of permanent account number; (ii) in the return of income'. Furthermore, every person who has a PAN number, and is entitled to an Aadhaar, must provide it to the relevant authority by a date to be specified (s. 139AA(2)). Failure to do so would mean that the PAN number 'shall be deemed to be invalid' (s. 139AA(3)). Counsel before the Supreme Court has described invalidation of PAN numbers as 'civil death', so great is their importance in Indian life. In effect, this legislation made obtaining an Aadhaar compulsory for most Indian citizens and residents, including any involved in businesses or professions.

The Supreme Court, in the 2015 *Puttaswamy Case*, had ruled that 'production of an Aadhaar card will not be condition for obtaining any benefits otherwise due to a citizen' and that the

---

[117] *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016* <https://uidai.gov.in/images/the_aadhaar_act_2016.pdf>

[118] UIDAI 'State/UT wise ranking based on Aadhaar saturation as on 15th May, 2017' <https://uidai.gov.in/images/state_wise_aadhaar_saturation_as_on_22052017.pdf>

[119] Various Aadhaar Act Regulations, 2016 < https://uidai.gov.in/legal-framework/acts/regulations.html>.

[120] Amber Sinha 'Analysis of Key Provisions of the Aadhaar Act Regulations', 31 March 2017, Center for Internet & Society < https://cis-india.org/internet-governance/blog/analysis-of-key-provisions-of-aadhaar-act-regulations>.

'Unique Identification Number or the Aadhaar card will not be used by the [central government] for any purpose other than the PDS Scheme [public distribution scheme] and in particular for the purpose of distribution of foodgrains, etc. and cooking fuel, such as kerosene. The Aadhaar card may also be used for the purpose of the LPG Distribution Scheme' (see above article 'Confusion as Indian Supreme Court Compromises …'). This was, however, before the *Aadhaar Act* was enacted in 2016, s. 7 of which states that the Central Government or a State Government may 'for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service' paid from central government funds 'require that such individual undergo authentication, or furnish proof of possession of Aadhaar number' (see above article 'Your Money or Your Life?').

In a temporary setback[121] for the PAN number aspect of the government's program to make the Aadhaar mandatory for all, the Supreme Court in *Viswam v Union of India*[122] in June 2017 has partially stayed the operation of s. 139AA. The bench of Justices A.K. Sikri and Ashok Bhushan has upheld the validity of s. 139AA, but has done so in a way which does not prejudice the outcome of the constitutional challenge to the Aadhaar on privacy grounds under Art. 21 of the Constitution, which has been referred to a 'constitution bench' of the Supreme Court.

The Court in *Viswam* made orders to the following effect:

(i) Because the question of the constitutionality of a compulsory ID number/card is still under review by a constitutional bench, on the basis of the alleged privacy rights under Constitution Art. 21, the court said 'we are not touching upon the privacy issue while determining the question of validity of the impugned provision of the Act'.

(ii) Therefore, the provisions in s. 139AA which in effect make it mandatory for a person without an Aadhaar to apply for one in order to obtain a PAN, and which make it mandatory for all PAN holders to provide an Aadhaar at some future date, must be inoperative until the constitution bench makes its decision.

(iii) However, for those who have already obtain an Aadhaar, it is valid for s. 139AA to require its production, in order to obtain a PAN, or to the file a tax return. Even if the *Aadhaar Act* does make obtaining an Aadhaar voluntary for some purposes, there is nothing inconsistent in the *Income Tax Act* making it compulsory for other purposes, because 'they operate in distinct fields.'

(iv) Section 139AA was consistent with other constitutional provisions, but this validity is contingent upon the conclusions of the constitution bench in relation to Art. 21.

As a result, the Modi government's attempt to make the Aadhaar compulsory for everyone with a PAN number seemed to have failed for the time being. But for those who have an Aadhaar, its use has been made mandatory from 1 July 2017 for filing tax returns, opening of bank accounts, and for financial transactions over Rs 50,000.

However, a week after Court's 9 June decision, it emerged that the Modi government's Finance Ministry had already issued new rules requiring existing bank account holders to submit Aadhaar details to banks by December 31, 2017, failing which the accounts will 'cease to be operational'.[123] This enables the government to subvert the Supreme Court's order: it cannot

---

[121] Staff 'Aadhaar-PAN linking: Setback for govt as Supreme Court partially stays making it mandatory', *FirstPost*, 9 Une 2017.

[122] *Binoy Viswam v Union of India (Writ Petition (Civil) No. 247 of 2017 & Ors)* Supreme Court of India, 9 June 2017 <https://uidai.gov.in/images/news/Supreme_Courts_Order_in_WP_247_277_304_of_201716062017.pdf>.

[123] Bureau 'Aadhaar made mandatory for new bank accounts, transactions above ₹50,000' *The Hindu – Business Line*, 16 June 2017 <http://www.thehindubusinessline.com/economy/aadhaar-made-mandatory-for-opening-bank-accounts-transactions-of-rs-50000-and-above/article9728579.ece>

cancel the PAN of those without an Aadhaar, but it can 'cancel' their whole bank account. No legal challenge to these rules is yet known.

No end to the saga of the Aadhaar is yet in sight, because the Chief Justice has not yet appointed the constitution bench of at least five justices which will hear the challenge to the Aadhaar legislation under s. 21 of the Constitution.

16. Privacy in the Other Seven South Asian (SAARC) States

While development of privacy protection has been paralysed in India, it is also stalled in the rest of South Asia for many other reasons. While there are no significant updates on data privacy laws for any of the parts of this Chapter, there are significant developments in a number of countries (particularly Sri Lanka) in relation to Right to Information (RTI) laws, and some political and other developments important to note in relation to potential longer-term developments. The South Asia / SAARC region therefore continues to be the Asian sub-region with the least development of data privacy laws.

Nepal

Nepal replaced its 2007 Interim Constitution with a new Constitution in 2015, amidst violent protests across the southern Tarai plains by ethnic groups, and dissatisfaction by other groups who consider they have been marginalised. Subsequent amendments in 2016 have not satisfied dissident groups.[124] Nevertheless, Nepal does have a constitution for the first time in nearly a decade. Devastating earthquakes in early 2015 have impeded progress in other areas.

UNESCO implemented an EU-funded project (to 2016) to make Nepal's *Right to Information Act 2007* more effective, and reported that the National Information Commission (NIC) had received 470 appeals from different information seekers, and has issued the order to public agencies to provide information to 409 of these appeals, but that NIC orders were not observed in all cases.[125] The have been no specific developments on data protection issues.

Bangladesh

There have been no data privacy developments in Bangladesh since 2014. The Right to Information law has been actively implemented by the Information Commission, which from 2009 to 2015, received 1,450 complaints about non-receipt of requested information, almost all of which had been finalised by 2016.[126]

Pakistan

In April 2017 Pakistan's IT Minister announced that the Ministry of Information Technology and Telecommunication (MoITT) would introduce a Data Protection Act (DPA) to Parliament 'within three months' in order to protect the rights of internet users.[127] Such claims are easy to make and break. A Privacy International report notes the provisions of the *Prevention of Electronic Crimes Act* 2016 which make it easier for police agencies to invade privacy.[128]

In February 2017 a Pakistan Senate select committee, which had been deliberating since 2012, approved for transmission to the Parliament a Right to Information (RTI) Bill to replace

---

[124] Crisis Group 'Nepal's Divisive New Constitution: An Existential Crisis' 4 April 2016 <https://www.crisisgroup.org/asia/south-asia/nepal/nepal%E2%80%99s-divisive-new-constitution-existential-crisis>

[125] UNESCO EU project EIDHR/2012/292-704 project report <http://www.unesco.org/new/en/kathmandu/communication-and-information/eu-right-to-information-project/>

[126] Muhammad Zamir 'Evolving Dimensions of the Bangladesh RTI Act' 3 November 2016, freedominfo.org website

[127] Maheen Karwai 'IT Ministry to introduce Data Protection Act in Pakistan within three months', Techjuice, 6 April 2017.

[128] Privacy International 'State of Privacy: Pakistan', 14 March 2017 <https://www.privacyinternational.org/node/970>.

the Freedom of Information Ordinance 2002 which has uncertain scope and effectiveness.[129] The provincial assembly in Sindh passed the *Sindh Transparency and Right to Information Bill, 2016*,[130] which will become an Act with its assent by the governor, and will repeal The Sindh Freedom of Information Act 2006.[131] A Sindh Information Commission will be established.

Sri Lanka

With the demise of the authoritarian Mahinda Rajapaksa government in an unexpected presidential election defeat in 2015, and a subsequent second defeat in Parliamentary elections, the prospects for data privacy laws in in Sri Lanka under the new Sirisena government have improved. The Sirisena government has aimed to implement a more parliamentary and less presidential government.

Sri Lanka's *Right to Information Act*[132] came into force on 4 February 2017. The RTI Act also establishes a Right to Information Commission.[133] The Act covers all public authorities, with a very broad definition of same (s. 43). The RTI Act has protections against the disclosure of personal information from government records, but only if the information is less than ten years old (s. 5). The Commission consists of five members appointed by the President upon the recommendation of the Constitutional Council, for five year terms (s. 12), and with other indicia of independence. The Commission has considerable powers, including to determine appeals against decisions by agencies (s. 15). Subsequent appeals can go to the Court of Appeal (s. 34). Every public authority must appoint an information officer, to whom individual make requests for information in the first instance (s. 23). This RTI Act is a very straight-forward 'access to documents' Act, and does not have any of the privacy-protective provisions of Nepal's similarly-named legislation, not even correction of inaccurate personal records. However, in establishing an independent Commission in this area, it provides one possible path for expansion to deal with data privacy issues (at least concerning public authorities).

The government's previous approach on data protection was that it is 'is pursuing a policy based on the adoption of a Data Protection Code of Practice, encompassing the private sector, with the possibility of the code being placed on a statutory footing through regulations issued under the Information and Communication Technology Act of 2003.[134] As such, this approach can be seen as self- or co-regulatory approach.'[135]

However, the Information and Communication Technology Authority's (ICTA) legal adviser described the prospects for enactment of a Data Protection Act as 'very positive', particularly in light of the establishment of the RTI Act and Commission. He said there was a need to 'look whether we could make use of Information Commissioner's Office to take additional requirements to monitor and implement' data protection.[136]

---

[129] Staff 'Pakistan parliamentary body approves Right to Information Bill', *The Indian Express*, 14 February 2017

[130] *Sindh Transparency and Right to Information Bill, 2016* (Pakistan) <http://shehri.org/rti/foi%20laws/Sindh%20Transparency%20&%20Right%20To%20Information%20Bill%202016.pdf>

[131] Habib Khan Ghori 'Sindh Assembly passes transparency, right to information bill', Dawn (newspaper), 14 March 2017.

[132] *Right to Information Act* (Act No. 12 of 2016) (Sri Lanka) <https://www.parliament.lk/uploads/acts/gbills/english/6007.pdf>

[133] RTI Commission website <https://www.parliament.lk/get-involved/right-to-information> .

[134] *Information and Communication Technology Act of 2003* (Sri Lanka) <https://www.gov.lk/elaws/wordpress/wp-content/uploads/2015/07/Information_and_Communication_Technology_Act_No.27.pdf

[135] Government of Sri Lanka *Analysis of e-Laws* (for Cybercrime Convention) <https://www.gov.lk/elaws/wordpress/CMSWrapper/content/elaws?appcode=cp&lang=en&gen_from=hme>

[136] CICRA Holdings website 'Data Protection Act implementation looks positive: Jayantha', undated, 2016 <http://www.cicra.lk/data-protection-act-implementation-looks-positive-jayantha/> ; interview with Jayantha Fernando.

Maldives

The Ministry of Economic Development of the Maldives put out a tender in May 2017 for 'Translation of Privacy and Personal Data Protection Act',[137] but there have been no other announcements about such plans.

Bhutan

The *Bhutan Information Communications and Media Bill 2016*[138] was passed by the National Assembly in June 2017, but must still be submitted to the National Council, with enactment possibly delayed until 2018.[139] The Bill contains extensive and complex provisions related to data privacy which, if enacted, will give Bhutan a data privacy law according to the criteria used in this book, but one which is restricted to provision of ICT services and to consumer e-commerce, whether provided by the private or public sectors. A brief summary only is given here.

Chapter 17 'Protection of online or offline privacy' requires organisations to protect personal information received from users or consumers, including sensitive personal information (which is defined). They must have an accessible privacy policy which sets out the purposes for which information may be collected and used, and details of rights of access and correction. Collection, use and disclosure are limited to 'that which a reasonable person would consider appropriate in the circumstances'. Users can require information to be removed. Organisations may only disclose information to third parties for these purposes (with an 'opt-in' exception for other uses), must ensure by contractual and other means that such third parties observe these requirements, and remain liable for their actions if they do not.

Chapter 21 of the Bill, 'Data Protection' sets out quite a comprehensive data privacy code which in some places repeats what is in Chapter 17, but often in a more strict form, and with more clarity in relation to offences and compensation. The chapter heading seems to limit it to data collected electronically. Collection, processing, and disclosure of personal information requires written permission or authority of law. Organisations must be 'delete or destroy all personal information which becomes obsolete'. Failure to protect data by 'reasonable security practices', unlawful disclosure of data, and unlawful copying of data, all constitute offences and liability to pay compensation.

The Bill also establishes an independent Bhutan Infocomm and Media Authority, and an Office of Consumer Protection, which have powers to investigate and resolve complaints, with rights of appeal to an appellate tribunal and then to the courts.

Afghanistan

The ongoing war in Afghanistan makes the prospect of any data privacy laws unrealistic.

---

[137] Tender documents (Maldives) < http://www.trade.gov.mv/dms/325/1494911558.pdf>,

[138] Bhutan Information Communications and Media Bill, 2016 (Bhutan) <http://www.nab.gov.bt/assets/uploads/docs/bills/2016/FinalBICMAbill2016Eng.pdf>

[139] Sonam Yangdon 'Bhutan Information Communication and Media Bill passed in the NA' *The Bhutanese*, 10 June 2017 <http://thebhutanese.bt/bhutan-information-communication-and-media-bill-passed-in-the-na/>.

PART III. REGIONAL COMPARISONS, STANDARDS, AND FUTURE DEVELOPMENTS

17. Comparing Protections and Principles—An Asian Privacy Standard?

There are no updates to the tables in this chapter – see the Chapter 20 overall update.

18. Assessing Data Privacy Enforcement in Asia—Alternatives and Evidence

There are no updates to the tables in this chapter – see the Chapter 20 overall update.

19. International Developments—Future Prospects for Asia

See Chapter 2 update for recent international developments, and Chapter 20 overall update.

20. Asian Data Privacy Laws—Trajectories, Lessons, and Optimism

In mid-2014 this book concluded with 'cautious optimism' about Asian data privacy laws, based on conclusions reached in the four chapters in Part III. A brief re-assessment is appropriate after three years. Overall, the conclusion of cautious optimism about improved laws and enforcement remains, but against a background of more rapidly increasing dangers from both state surveillance and private sector surveillance capabilities through data analytics and its expanding access to personal data because of social media, the Internet of things, open government data, and numerous other technical developments.

Jurisdictions with laws

There has been a small but not a dramatic expansion of the jurisdictions with data privacy laws. Indonesia now has laws with all of the elements of a basic data privacy law, and incremental changes to China's laws leave it very close to a similar status, except for uncertainties concerning individuals' access to their records, and the scope of private sector coverage. In practice, the Philippines' law was dormant, and is now active. There is the prospect of a new law in Bhutan, but again with questions of breadth of scope, and there are promising signs in Sri Lanka. That still leaves almost half the 26 countries of Asia where the prospects are not very encouraging for enactment of data privacy laws.

Principles

Reforms strengthening privacy principles are most notable in Japan (from a low base), but have also been present in Indonesia (where a much stronger Bill awaits Parliamentary consideration), Korea and Taiwan.

In Japan and Korea, while their approaches to 'big data' / de-identification may undermine some aspects of their privacy protections, both countries are attempting to deal with issues that other countries will have to address. There is a danger that India will be found to have no constitutional right to privacy, increasing the authoritarian potential of the Aadhaar, and making a worthwhile data privacy law less likely. The data localisations laws in China and elsewhere are not a threat to privacy, whatever else might be thought of them. Attempts to destroy data export restrictions and data localisation provisions have failed as yet with the

demise of the Trans-Pacific Partnership (TPP), and it is unknown what RCEP will offer in that regard.

Enforcement

Enforcement continues to strengthen across Asia, but not dramatically. The Korean Communications Commission (KCC) has set a high benchmark with a penalty of US$4.5 million (approximately) against a Korean company. In two cases, Taiwan's financial regulator has issued fines of around US$100,000. Singapore's PDPC has imposed one fine of US$35,000 and others of half that amount. Other than for Korea and Taiwan, financial penalties in Asian jurisdictions still fall far short of the dissuasive effect of the six figure penalties that are now becoming common in Europe. Other significant aspects of enforcement are the frequent use of criminal sanctions, including imprisonment, for fraudulent sale or purchase of personal data in China, and the recommendation of prosecutions by the newly-appointed Philippines DPA. Japan's law does now include some enforcement powers, but they are only in effect in mid-2017 and it is not known if they will be used.

Comparisons with international standards

In 2014 the eleven Asian countries with data privacy laws (which included China for this purpose) were assessed against the ten 'European' privacy standards (principles and enforcement requirements) which distinguish the 1995 EU data protection Directive from the 1980 OECD Guidelines. The result was that those countries, on average, implemented 5.4 of those 10 'European' standards in their laws, and were in that sense marginally 'closer' to the EU standard than the OECD standards. Since 2014, the amendments to Japan's law, and Singapore's data export regulations, strengthened this average somewhat (to 5.7), but this is offset by the need to add Indonesia's minimal new law, so that the overall average is still 5.4. Asian data privacy laws remain approximately half-way between the EU and OECD standards.

International engagement

Since 2014, Asian jurisdictions have become more involved with international data privacy standards and organisation. Korea and Japan are both seeking to be the first countries in Asia to receive a positive adequacy assessment from the EU. The Philippines, Indonesia, Japan and Korea have all obtained observer status on the Consultative Committee of Council of Europe data protection Convention 108, and have attended annual Plenary meetings. At present, Convention 108's non-European members (and proposed accessions) are all from Africa or Latin America, and its development as a global privacy treaty would be enhanced greatly by accessions from the Asia-Pacific region. No non-OECD countries in Asia have taken up the invitation to accede to the 2013 revised OECD Guidelines. The appointment of a UN Special Rapporteur on the Right of Privacy has not yet had any clear impact in Asian jurisdictions, but it is only a recent (2015) appointment. Japan has become the second full participant in the APEC CBPRs (with the USA), and Korea has completed all steps except selection of an Accountability Agent. Other countries have indicated intentions to become involved but have not yet taken any of the steps required to do so. Asian countries have also participated actively in the Global Privacy Enforcement Network (GPEN), and in APEC's Cross Border Privacy Enforcement Arrangement (CPEA).